Product Guide

McAfee Security for Microsoft SharePoint 3.0.0

COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1 Introduction 7

Product features . . . 7
How it protects the SharePoint server . . . 8

2 Installation 11

Pre-installation . . . 11
System requirements . . . 11
User roles . . . 12
Prerequisites . . . 13
Types of installation . . . 14
Standard installation . . . 14
Upgrade from previous version . . . 15
Post-installation . . . 16
Testing your installation . . . 16
Test the on-access scanner . . . 16
Test the on-demand scanner . . . 16
Installed components and services . . . 17

3 Dashboard 19

Statistical information of the detected items . . . 19
Detections . . . 20
Scanning . . . 22
Graph . . . 22
Product versions and updates . . . 23
Update information . . . 24
Schedule a software update . . . 24
Product information . . . 25
Licenses . . . 25
View recently scanned items . . . 26
On-Demand scan . . . 26
Viewing On-demand scan tasks . . . 28
Create an on-demand scan task . . . 29
Graphical reports . . . 31
View graphical reports using simple search filters . . . 31
View graphical reports using advanced search filters . . . 32

4 Detected items 35

Primary search filters . . . 35
Additional search options . . . 36
Search detected items . . . 36
Actions that you can take on quarantined items . . . 37

5 Policy Manager 39

Policy manager menu options . . . 39
Policy categories to handle threats . . . 40

Policy manager views . . . 40
Master policy and sub-policy . . . 41
Create sub-policies . . . 42
Core scanners and filters . . . 43
List all scanners and filters for a selected policy . . . 43
Add a scanner or filter . . . 44
Create policy rules . . . 45
Actions you can take on detections . . . 46
Shared resource . . . 46
Configure scanner settings . . . 46
Configure alert settings . . . 47
Create a new alert . . . 48
Configure DLP and Compliance rules . . . 50
Configure file filtering rules . . . 52
Configure time slots . . . 53
Manage core scanner settings for a policy . . . 54
Configure anti-virus scanner settings . . . 55
Configure file filtering settings . . . 57
Configure DLP and Compliance scanner settings . . . 58
Manage filter settings for a policy . . . 60
Configure corrupt content settings . . . 60
Configure protected content settings . . . 61
Configure encrypted content settings . . . 61
Configure signed content settings . . . 62
Configure password-protected files settings . . . 62
Configure scanner control settings . . . 63

6 Settings and diagnostics 65
Configure local quarantine database for detected items . . . 66
User interface preference settings . . . 67
Configure dashboard settings . . . 67
Configure graph and chart settings . . . 68
Diagnostics settings . . . 69
Configure debug log settings . . . 69
Configure error reporting settings . . . 70
Configure event log settings . . . 71
Configure product log settings . . . 71
View product logs . . . 73
Import and export configuration settings . . . 74
Import product configuration from another server . . . 75
Export your product configuration . . . 75
Import a sitelist . . . 76
Configure DAT settings . . . 76
Configure user settings . . . 77

7 Program Maintenance 79
Repair the installation . . . 79
Purge and optimize . . . 80
Restore default configuration . . . 81
Uninstall the software . . . 81

8 Integrating with ePolicy Orchestrator 83
Prerequisites . . . 83
Check in the software package . . . 84
Install the software extensions . . . 84
Migrate the policies from older version . . . 84

Deploy the software to clients . . . 85
Manage Policies . . . 86
Create or modify policies . . . 86
Assign policies . . . 87
Create and schedule tasks . . . 87
Schedule automatic updates . . . 88
Schedule on-demand scan . . . 89
Schedule an optimization task . . . 89
Schedule purge old DATs task . . . 90
Schedule purge task . . . 91
Queries and reports . . . 91
Predefined queries . . . 91
Run a default query . . . 92
Filter events . . . 93
Remove the software . . . 94
Remove the software from client systems . . . 94
Remove the software extensions . . . 95

A Creating a customized domain user account with the least SQL permissions 97

B SiteList Editor 101
Configure sitelist proxy settings . . . 102
Configure sitelist repository settings . . . 103

C Using access control 105

Index 107

Contents

1 Introduction

McAfee® Security for Microsoft SharePoint protects the data stored on your Microsoft SharePoint server from various threats that could adversely affect the computers, network, or employees.

It scans all files that you upload or download from the SharePoint server. It uses advanced heuristics against viruses, unwanted content, potentially unwanted programs, and banned file types. You can configure the actions to take on the detected and the suspicious items.

Contents

- *Product features*
- *How it protects the SharePoint server*

Product features

The main features of McAfee Security for Microsoft SharePoint are:

- **Protection from viruses** — Scans all the content for viruses and protects your SharePoint server by intercepting, cleaning, and deleting the viruses that it detects. It uses advanced heuristic methods and identifies unknown viruses or suspected virus-like items and blocks them.
- **Capability to detect packers and potentially unwanted programs** — Detects packers that compress and encrypt the original code of an executable file. It also detects potentially unwanted programs (PUPs), that are software programs written by legitimate companies to alter the security state or privacy state of a computer.
- **Integrate with McAfee® ePolicy Orchestrator® (McAfee ePO™) 4.5, 4.6 and, 5.0** — Integrates with the ePolicy Orchestrator server to provide a centralized method for administering and updating the software across your SharePoint servers. This reduces the time required to administer and update various systems.
- **McAfee Global Threat Intelligence Technology (GTI)** — Safeguards your SharePoint server by providing real-time security from the ever-evolving threats even before a signature or DAT update is available.

  When a suspicious file is detected on a managed node protected by a McAfee anti-malware product with GTI, it connects to McAfee servers in real-time and checks against the database. If the suspicious file is found to be malicious, the managed node is notified and protected. The query and response happens in milliseconds.

  See the McAfee KnowledgeBase article KB68631 for more information.
- **Support for incremental on-demand scans** — Incremental on-demand scans saves time by scanning only the newly added documents in the SharePoint server without re-scanning the entire server.
- **Support for resumable scans** — Scans the documents and folders from the last scanned folder. McAfee Security for Microsoft SharePoint saves the state of the scan. When the same task is started later, the scan resumes from the last scanned folder.

- **DLP and Compliance** — Scans the textual data in documents. Ability to ensure that the content is in accordance with confidentiality and compliance policies.

  Pre-defined compliance dictionaries include:

  - Addition of 60 new DLP and Compliance dictionaries.
  - Support for industry specific compliance dictionaries — HIPAA, PCI, SourceCode (Java, C++ etc.)
  - Improvements to existing phrase based detections.
  - Reduced false positives, due to enhanced capabilities in detecting non-compliant content, based on the Threshold score and in combination with the maximum term count (occurrence).

  Customize policies for content security and Data Loss Prevention (DLP).
- **Support for virtual environment** — This release is supported in virtual environment such as VMware Workstation 7.0 or later and VMware ESX 5.x.
- **Support for upgrade** — Upgrade from McAfee Security for Microsoft SharePoint 2.5 Patch1 to McAfee Security for Microsoft SharePoint 3.0 (both standalone and through ePolicy Orchestrator).
- **Web-based user interface** — Provides a user-friendly web-based user interface.
- **Quarantine management** — Specify local database to quarantine the infected documents. You can search the database to get data on the infected documents.
- **Reports** — View the reports on various scans from the main dashboard in graphical form.

How it protects the SharePoint server

McAfee Security for Microsoft SharePoint integrates with your SharePoint server and scans all the documents on the SharePoint server.

When the user uploads the documents, SharePoint passes the documents to McAfee Security for Microsoft SharePoint.

- The anti-virus scanning engine compares the documents with all the known virus signatures stored in the DATs.
- The DLP and Compliance engine scans the documents for banned content as specified in the content management policies.

Scanning takes place each time you create, save, or modify data on the SharePoint server. You can also schedule scans to run immediately, at a particular time, or at regular intervals.

Real-time detection

The software checks the documents and files in real time against the repository of up to date DAT files, malware and malicious content. If it finds the files to be malicious, it notifies and protects the managed node. It leverages the McAfee GTI technology to prevent damage and data theft even before a signature or a DAT update is available.

Scheduled detection

You can schedule scans that start manually or at regular intervals. The software checks all the files uploaded against the latest set of virus signatures and content management policies.

Scanning the documents and folders on the SharePoint server

- The anti-virus and the content scanning engines scan the documents and provide the result to McAfee Security for Microsoft SharePoint before the content is written on to the Microsoft SharePoint server.
- The anti-virus engine compares the documents with all the known signatures stored in the currently installed virus definition files (DATs).
- The content scanning engine scans the documents for banned content as specified in the content management policies running within the software. If there are no viruses, banned/unwanted content in the documents, it passes the information back to SharePoint server. In case of a detection, the software takes actions as defined within its configuration settings.

What and when to scan?

- The threat from viruses can come from many directions such as infected macros, shared program files, files shared across a network, floppy disks, files downloaded from the internet, and so on. Individual McAfee Security for Microsoft SharePoint anti-virus software products target specific areas of vulnerability.
- McAfee Security for Microsoft SharePoint provides a range of options that you can further configure according to the demands of your system. These demands will vary depending on when and how the component parts of your system operate and how they interact with each other and with the outside world.
- You can configure or enable various actions that allow you to determine how your Microsoft SharePoint server should deal with different items and what actions it should take on detected or suspicious items.

2 Installation

Includes important information to be considered before, during and post installation..

Contents

- *Pre-installation*
- *Types of installation*
- *Post-installation*

Pre-installation

Use this information to prepare for the product installation.

System requirements

Make sure that your server meets these requirements.

Component	Requirements
Processor	• Intel x64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T) • AMD x64 architecture-based processor with AMD 64-bit technology
Memory	The memory requirement to install this product is the same as Microsoft SharePoint server system requirement. For more information, see the Microsoft SharePoint website. • Microsoft SharePoint server 2007 — 4 GB RAM • Microsoft SharePoint server 2010 — 8 GB RAM • Microsoft SharePoint server 2013 — 8 GB RAM
Available hard disk space	Minimum 740MB of free hard disk space where Microsoft SharePoint is installed
Operating system	• Microsoft Windows 2008 Standard/Enterprise Server SP2 (64-bit) • Microsoft Windows 2008 Standard/Enterprise Server SP1 R2 (64-bit) • Microsoft Windows 2012 Standard/Enterprise Server R2 (64-bit)

Component	Requirements
Microsoft SharePoint server	• Microsoft Office SharePoint Server 2007 /Windows SharePoint Services 3.0 (64-bit) • Microsoft SharePoint Server 2010 /SharePoint Foundation server 2010 (64-bit) • Microsoft SharePoint Server 2013 /SharePoint Foundation server 2013 (64-bit)
Browser	• Microsoft Internet Explorer version 8.0, 9.0, and 10.0 • Mozilla Firefox version 20.x and 21.x McAfee Security for Microsoft SharePoint is certified for Internet Explorer and FireFox. You can use other browsers, however they are not tested.
Screen resolution	1024x768 resolution or higher (recommended)
McAfee management software	• McAfee ePolicy Orchestrator 4.5 • McAfee ePolicy Orchestrator 4.6 • McAfee ePolicy Orchestrator 5.0
McAfee® Agent (required for McAfee ePO deployment)	McAfee Agent 4.6 and later
Network	10/100/1000Mbps Ethernet card

User roles

These are the user roles associated with McAfee Security for Microsoft SharePoint.

Role	Description
SharePoint Farm administrator (full permissions)	Domain account with full administrator permissions for all Windows servers and farm level services in the SharePoint server farm. This account needs to be specified during the McAfee Security for Microsoft SharePoint installation.
SharePoint administrator (full permissions)	Domain account with full administrator permissions for SharePoint installed on a single server. This account needs to be specified during the McAfee Security for Microsoft SharePoint installation.
Custom user (minimum permissions)	Domain account with the minimum permissions/least privileges required for the product to run. This account needs to be specified during the McAfee Security for Microsoft SharePoint installation. See the section *Creating a customized domain user account with the least SQL permissions* for instructions.
Windows administrator	Account that is a member of local administrator's group to launch the McAfee Security for Microsoft SharePoint installer. This might be the same as the farm administrator account if being used for installing the product. However, if the custom user is being used to run McAfee Security for Microsoft SharePoint, you need a Windows administrator account to run the installer.
ePolicy Orchestrator administrator	To deploy, manage, and administer McAfee Security for Microsoft SharePoint from ePolicy Orchestrator server.

Prerequisites

Before installing the product, make sure that your client system is ready and meets all requirements.

SharePoint installation in single server mode

When the SharePoint server is installed in a single server mode, here's a checklist of instructions you can use before installing McAfee Security for Microsoft SharePoint.

- Make sure you have the Windows administrator credentials to install McAfee Security for Microsoft SharePoint. This account must be a member of Windows administrator's group and the credentials are required for launching the product installer.
- Make sure you have the SharePoint administrator credentials to supply to the McAfee Security for Microsoft SharePoint installer. This account must be a member of the local administrator group on the SharePoint server and database server for remote database access.
- If you're upgrading from a previous release, uninstall any earlier versions of the product other than McAfee Security for Microsoft SharePoint 2.5 patch 1.
- Choose an open/unused port on the server where you want to host the software site. You can use the default port 45900 if available. Telnet a port using the Windows command prompt to check if it is open.

From a remote server, use the command telnet <host name or IP address> <Port>.

- Connection refused means that the port is available (open).
- Accepted means that the port is in use and not available.
- Timeout means that a firewall is blocking the access. From the same server, use `netstat –an` to check to see if 45900 port is listening.

SharePoint installation in a farm

These are the actions you must perform before installing McAfee Security for Microsoft SharePoint when the SharePoint server is installed in a farm.

McAfee recommends that you install McAfee Security for Microsoft SharePoint with SharePoint Farm administrator credentials. The software should be installed on the following servers within the server farm:

- All Web Front-End (WFE) servers that host Portal sites.
- All WFE servers that host Windows SharePoint Services team sites.
- When a WFE server redirects traffic to another SharePoint role in the farm, McAfee Security for Microsoft SharePoint must be installed on both the WFE server and the destination SharePoint role. This is because the redirected traffic does not pass through McAfee Security for Microsoft SharePoint on the WFE.

McAfee Security for Microsoft SharePoint is not required on the server types below:

- Application servers

When you configure on-demand or scheduled scans in an environment where McAfee Security for Microsoft SharePoint is not installed on the application servers, the entire database contents are retrieved from the application servers and streamed over the network to the WFE for scanning. In such cases, it can be beneficial to install McAfee Security for Microsoft SharePoint locally on the application servers to minimize bandwidth usage.

- Search Servers

- Index Management Servers

If you choose to install McAfee Security for Microsoft SharePoint on an Indexing Server, make sure that indexing is scheduled to occur during off-peak hours to minimize the impact of on-access scanning on server performance.

- Job Servers
- Microsoft SQL Servers

If your organization's policy restricts you from using SharePoint Farm administrator credentials or if you do not want to use them for other reasons, you can create a customized normal domain user account with minimum permissions needed for McAfee Security for Microsoft SharePoint to run. See the section *Creating a customized domain user account with the least SQL permissions* for instructions.

Types of installation

McAfee Security for Microsoft SharePoint can be installed on a standalone server or deployed using ePolicy Orchestrator.

See also

Integrating with ePolicy Orchestrator on page 4

Standard installation

During standard installation, a wizard appears leading the installation process through a series of instructions you must follow.

Task

1. To install the McAfee Security for Microsoft SharePoint, download the `MSMS30_EN.zip` (for English) archive and extract the files to a temporary location on your system.
2. Double-click `setup.exe`. If the software is a licensed version, the **McAfee End User License Agreement** dialog box appears.
3. From the drop-down lists, select the license expiry type and the location from where you purchased the software.
4. Accept the terms in the license agreement, then click **OK**.

   The software installation wizard appears leading the installation process through a series of instructions you must follow.
5. Click **Next**.
6. McAfee Security for Microsoft SharePoint is installed on the default port 45900. Specify a custom port on which the Microsoft Internet Information server must host McAfee Security for Microsoft SharePoint, then click **Next**.

   The **Destination Folder** dialog box appears.

7 Click **Next** to install the software in the default location `C:\Program files (x86)`.

- You can select a different location for installing the software by clicking **Browse**. Select another location, click **OK** to return to the installation wizard, then click **Next**.
- It is a good practice to have the McAfee Security for Microsoft SharePoint installed in the default directory of the system drive. However, you can select another location as per your requirement.

The **Database Account** dialog box appears.

8 Type your account name (domain or workgroup\username) and password, click **Next**.

9 Type the credentials of the system where SharePoint is installed. For example: Domain\UserName or Workgroup\UserName.

a The account credentials are validated by the server. The account must be a member of the local Administrator's group on the server on which you are installing McAfee Security for Microsoft SharePoint.

If the user credentials cannot be resolved by the server, a warning dialog box appears prompting you to check your credentials.

b Verify if you have entered correct credentials. Click **OK**, then click **Next** to override the warning and proceed with the installation process with unresolved account information.

The **Ready to Install the Application** dialog box appears.

You can use `SetSQLAct.exe` to modify your credentials in case of an incorrect entry while installing McAfee Security for Microsoft SharePoint. This utility is located in `<Installation folder>\bin`.

On the command prompt, type `SetSqlAct.exe /USER=<username> /PASSWORD=<password> /DOMAIN=<domain>`.

10 Click **Next**. A progress bar appears indicating the status of the installation process.

11 After the installation is complete, select or deselect the following options as needed and click **Finish**.

- **View Readme** — To read the software release notes that describes the product features, last-minute changes to the documentation, and any known behavior or other issues with the product.
- **Launch User Interface** — To launch the graphical user interface of the software. This will launch the product in standalone mode.
- **Update Now** — To download the latest product updates to ensure you are running the most current security to combat the ever-evolving threats. Your system must be connected to the Internet to receive automatic updates regularly.

McAfee Security for Microsoft SharePoint is now installed on your system.

Upgrade from previous version

McAfee Security for Microsoft SharePoint supports upgrade of the configuration settings from the previous version of the software.

When upgrading to a new version, you need not uninstall the existing version. The installation program updates your installation to the new version.

Upgrade is supported from the product version 2.5 Patch 1 to this release.

Task

1 As an administrator, log on to the system where Microsoft SharePoint server is installed.

2 From the setup folder of the extracted .zip archive, double-click `setup.exe`.

3 In the **Preparing to Install** screen, the installation wizard is prepared and all required installation files are extracted. The process is same as with the standard installation. See the section *Standard Installation*. When the process is complete, the **Changes completed** screen appears.

You have successfully upgraded to the latest version.

Post-installation

After you install McAfee Security for Microsoft SharePoint, we recommend that you test the software.

Testing your installation

After installing McAfee Security for Microsoft SharePoint, we recommend that you test the installation to make sure that the software is installed properly.

You can test the operation of the McAfee Security for Microsoft SharePoint software by running the *EICAR* Standard Anti-virus Test File on any computer where you have installed the software.

The EICAR Standard Anti-virus Test File is a combined effort by anti-virus vendors throughout the world to implement one standard by which customers can verify their anti-virus installations.

Test the on-access scanner

You can test the on-access scanner using the EICAR file.

Task

For option definitions, click **?** in the interface.

1 Launch the Microsoft SharePoint server.

2 Copy the following line into a file, save the file with the name `EICAR.TXT`:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

The file size is 68 or 70 bytes.

If you have any other security software installed on your server (such as McAfee VirusScan Enterprise), you must disable its scanner during this process. This is to prevent the file from being identified by another security software.

3 Start the McAfee Security for Microsoft SharePoint software and add the `EICAR.TXT` file to your Microsoft SharePoint server. The McAfee Security for Microsoft SharePoint on-access scanner action is configured to **Prevent Upload/Download of the Item** and hence the file is not saved on your SharePoint server.

Test the on-demand scanner

You can test the on-demand scanner by using the `EICAR.TXT` file.

For option definitions, click **?** in the interface.

Task

1 Launch the Microsoft SharePoint administration interface by clicking **Start** | **Programs** | **SharePoint Portal Server** | **SharePoint Central Administration**.

2 Click **Configure anti-virus settings** under **Security Configuration**.

3 Deselect **Scan documents on upload** and **Scan documents on download**.

4 Delete the previous copy of `EICAR.TXT` from the document store.

5 Add `EICAR.TXT` back into the document store. Schedule an on-demand scan for that document store. The McAfee Security for Microsoft SharePoint software reports finding the EICAR test file as per the default on-demand policy setting **Replace item with an alert**.

6 Delete the file when you have finished testing your installation to avoid alarming unsuspecting users.

7 Make sure that you enable on-access scanning to provide real-time protection against viruses and unwanted files and content within your SharePoint computer.

If you have disabled any other anti-virus software during these tests, make sure that you enable them.

Installed components and services

The software installs these components on your SharePoint server.

To access these components, click **Start** | **Programs** | **McAfee** | **McAfee Security for Microsoft SharePoint**, then click the component:

- **McAfee Auto Update Sitelist Editor** — Specifies the location where automatic updates (including DATs and scanning engines) are downloaded from.
- **MSMS (Mozilla UI)** — Launches the software standalone version through Mozilla Firefox browser.
- **MSMS (Web UI)**— Launches the software standalone version through the web browser.
- **Access Control** — Allows or denies access to the McAfee Security for Microsoft SharePoint user interface for specific users or groups.

Services available

- **McAfee Framework Service** — Prerequisite for installing and using ePolicy Orchestrator. For details on this service, see ePolicy Orchestrator product documentation.
- **McAfee Portalshield** — Protects your Microsoft SharePoint Server from viruses, unwanted content, potentially unwanted programs, and banned file types/messages.

3 Dashboard

Dashboard presents information in a way that is easy to interpret. It provides critical information on how well your server is being protected from viruses and unwanted content. It also provides information about the detection statistics; additional components installed in the product; version information of components such as engine and DAT files; product license information and recently scanned items.

Contents

- *Statistical information of the detected items*
- *Product versions and updates*
- *View recently scanned items*
- *On-Demand scan*
- *Graphical reports*

Statistical information of the detected items

Provides detailed information on the total items scanned by McAfee Security for Microsoft SharePoint, how many items triggered the detection and are quarantined based on the detection category. The dashboard also provides this statistical information in the form of a graph, for easy interpretation, and monitor the detection rates.

The **Statistics** are categorized into:

- **On-Access Settings**
- **Detections**
- **Scanning**
- **Graph**

On-Access Settings - Specifies if you want to scan the documents when they are uploaded or downloaded. This setting is linked to the SharePoint Anti virus central administration settings. We recommend that you always enable the **On-Access Settings**.

Clicking **Reset** will clear the statistical information of all counters in the **Detections** section and reset the value to zero. Resetting the statistics will not delete any quarantined items from the **Detected Items**. These counters are dependent on the database path, so if you change the database path under **Settings & Diagnostics** | **Detected Items** | **Local Database**, the counters will reset to zero.

To modify the dashboard settings such as the refresh rate; maximum items to appear in the **Recently Scanned Items**; graph scale units; graph and chart settings such as the 3D pie-chart, bar graph, exploded pie-chart, transparency, go to **Settings & Diagnostics** | **User Interface Preferences**.

Detections

Displays all statistical information on how many items scanned by McAfee Security for Microsoft SharePoint are clean and how many items triggered a detection. Based on the detection category, the respective counter is incremented.

The reported numbers indicate the number of items that trigger any of the detection methods.

If your McAfee Security for Microsoft SharePoint server is managed by ePO and if you restart the service or click the **Reset** button, these statistics will vary in ePO reports due to the historical data stored in ePO. For more information on ePO reports, see *Integrating McAfee Security for Microsoft SharePoint with ePolicy Orchestrator* chapter.

Table 3-1 Icons used — Detections section

Icon	Description
	Provides additional information on the detection category when you place the mouse pointer on the icon.
	Indicates that the statistics of the respective detection category is shown in the graph.
	Indicates that the statistics of the respective detection category is not shown in the graph.

The following table provides you more information on each detection category.

Table 3-2 Detection Definitions

Category	Additional information	Description
Clean	If there are more clean items than the detections, enabling this icon for clean items may suppress the graph of other categories. In such scenarios, disable the icon next to **Clean** category.	Legitimate items that do not pose a threat to the user and does not trigger any of the scanners.
Viruses		A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files, so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates files. Some viruses display symptoms, others damage files and computer systems, but neither is essential in the definition of a virus; a non-damaging virus is still a virus.
	Viruses detected	The number of the viruses that are detected in an item.
	Viruses cleaned	The number of the viruses that are cleaned from an item.
Potentially Unwanted Programs		Potentially Unwanted Programs (PUP) are software programs written by legitimate companies that could alter the security or privacy policies of a computer on which they have been inadvertently installed. These programs could be downloaded along with a legitimate application that you might require.
	PUP detected	The number of the PUP's that are detected in an item.

Table 3-2 Detection Definitions *(continued)*

Category	Additional information	Description
	PUP blocked	The number of the PUP's that are blocked from an item.
Banned File types/Messages		Certain types of file attachments are prone to viruses.
	Banned file types	The number of the banned file types that are detected in an item.
	Banned messages	The number of the banned messages that are detected in an item.
DLP and Compliance	To view available dictionaries, click the **Category** drop-down list from **Policy Manager** | **Shared Resource** | **DLP and Compliance Dictionaries**.	The software provides industry-leading content analysis to provide the tightest control of sensitive content in any form to aid compliance with many state, national, and international regulations. Prevent data leakage with the most extensive Data Loss Prevention (DLP) in the industry that does pattern matching to detect data; policy-based message handling that prevents outbound data loss.
	DLP and Compliance	The number of the DLP and Compliance detections in an item.
Unwanted Content		Unwanted Content is any content that the user would not like to be present on the server. The rules can be defined by certain words or phrases which would trigger a corresponding policy and block the document.
	Packers	A packed executable that decompresses and/or decrypts itself in memory while it is running, so that the file on disk is never similar to the memory image of the file. Packers are specially designed to bypass security software and prevent reverse engineering.
	Encrypted/Corrupted content	Documents that are categorized as having encrypted or corrupted content.
	Encrypted content	Some documents can be encrypted, which means that the content of those documents cannot be scanned.
	Signed content	Whenever information is sent electronically, it can be accidentally or willfully altered. If the document contains a virus, bad content, or is too large, the software might clean or remove some part of the message. The document is still valid, and can be read, but the original digital signature is broken. You cannot rely on the contents of this document because the content might also have been altered in other ways. Signed content policies specify how documents with digital signatures are handled.
	Corrupted content	The content of some files can become corrupt, which means that the content of the file cannot be scanned.
	Denial of service	A means of attack against a computer, server or network. The attack is either an intentional or an accidental by-product of instruction code that is either launched from a separate network or Internet-connected system, or directly from the host. The attack is designed to disable or shut down the target, and disrupts the system's ability to respond to legitimate connection requests. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests.

Table 3-2 Detection Definitions *(continued)*

Category	Additional information	Description
	Protected content	The content of some files is protected, which means that the content of these files cannot be scanned.
	Password protected files	The content of some files is protected by password. Password-protected files cannot be scanned.
	Incomplete MIME messages	Multipurpose Internet Mail Extensions (MIME) is a communications standard that enables the transfer of non-ASCII formats over protocols, like SMTP, that only support 7-bit ASCII characters. MIME defines different ways of encoding the non-ASCII formats so that they can be represented using characters in the 7-bit ASCII character set.
	Others	Any other detections that are not classified in the specified detection categories.

Scanning

Displays information on the total items scanned by McAfee Security for Microsoft SharePoint and the average time taken to scan all items, since the last reset.

Table 3-3 Option definitions

Option	Definition
Average Scan Time (milliseconds)	Specifies the average time taken by McAfee Security for Microsoft SharePoint to scan all the items that reach the SharePoint server. To understand how this is calculated, let's consider this example where: • T = Total time taken to scan all the items after the last McAfee PortalShield service restart. • N = Total number of items scanned after the last McAfee portalShield service restart. then, Average scan time = T/N (in milliseconds)
Total Scanned	Total number of items scanned, since the last time the statistic counters were reset.

Graph

Displays the statistics of the detections scanned by the software in a graphical format.

Table 3-4 Icons used — Graph section

Icon	Description
	View statistical information of the selected counters as a bar graph. This is useful when you want the statistics of total number of items scanned and the items that triggered a detection during the selected duration.
	View statistical information of the selected counters as a pie chart. This is useful when you want the percentage of items scanned and the items that triggered a detection during the selected duration.

Table 3-5 Option definitions

Option	Definition
Graph	• **Clean** — Provides information on how many items were clean for the selected time range. • **Virus** — Provides information on how many items were detected as virus by the software for the selected time range. • **Unwanted Content** — Provides information on how many items were detected as unwanted content by the software for the selected time range. • **Potentially Unwanted Programs** — Provides information on how many items were detected as potentially unwanted programs by the software for the selected time range. • **Banned File types/Messages** — Provides information on how many items were detected as banned file types/messages by the software for the selected time range. • **DLP and Compliance** — Provides information on how many items were detected as DLP and Compliance by the software for the selected time range.
Magnify Graph	Specify the magnification percentage of the **Detections** graph. This helps you view an enlarged graph, which is useful when the default graph in the dashboard is cluttered with more information and becomes unreadable in the current browser window.
Time range	Specify for which time period you would like to review the statistics. The available options are: • **Last 24 Hours** • **Last 7 Days** • **Last 30 Days**

Product versions and updates

Provides important information on whether the software is up-to-date with latest DATs and extra drivers. It also provides information about the product license type.

Versions and updates

The **Versions & Updates** section in the **Dashboard** has these tabs:

- **Update Information**
- **Product Information**
- **Licenses**

Update information

Provides information about anti-virus DAT and anti-virus engine version, their status and when they were last updated. McAfee Security for Microsoft SharePoint uses the McAfee update website or McAfee ePO to automatically update its anti-virus DAT, engine and rules on a daily-basis.

Table 3-6 Option definitions — Update Information

Option	Definition
Last Successful Update	Displays the time when the software was updated successfully.
Update Now	Click to immediately update the product with latest engine and drivers. This is helpful in a situation when there is a virus out-break and you cannot wait until the scheduled software update occurs. — Indicates that your anti-virus DAT is up to date. — Indicates that the your anti-virus DAT is out of date.
Update Frequency	Displays the schedule frequency of how often the software is updated.
Edit Schedule	Click to schedule or edit the product's software update. For more information on how to update the software, see *Schedule a software update* section.
Show Status	Click to view the current status of the update task such as the start time, running time, current status and how much the task has progressed. You can see the status of the current update. To view the status of the previous updates from **Settings & Diagnostics** | **Product Log**.
Anti-Virus Engine | DAT Version | Extra Drivers	Displays the latest anti-virus engine, DAT version and extra drivers information and when it was updated.
Viruses that Extra Drivers Detect	Displays items that were detected by ExtraDAT to remove particular viruses. `EXTRA.DAT` files contain information that is used by the software to detect a new virus. When a major virus is discovered and extra detection is required, an `EXTRA.DAT` file is made available until the normal DAT update is released.

Schedule a software update

Keep your software up-to-date with the latest anti-virus DAT and anti-virus engine by scheduling an automatic update.

Task

For option definitions, click **?** in the interface.

1 Click **Dashboard** | **Statistics & Information**.

2 From the **Versions & Updates** section, click **Update Information** tab.

3 From **Update Frequency**, click **Edit Schedule**.

The **Edit Schedule** page appears.

4 From **Choose a time** tab, specify when you want to schedule an update. The available options are:

- **Not scheduled** — Select this if you have not decided on when to perform the update.
- **Once** — Specify the date and time to schedule an update once.
- **Hours** — Select this to schedule the update based on hours.
- **Days** — Select this to schedule the update based on how often the update must occur in a week.

- **Weeks** — Select this to schedule the update based on how often the update must occur in a month.
- **Months** — Select this to schedule the update based on how often the update must occur in a year.

- By default a daily update is scheduled. McAfee recommends that you don't change the default value.
- If the server is managed using McAfee ePO, the settings defined in McAfee ePO will take precedence over the local settings.

5 Click **Save**, then **Apply**.

You have now successfully scheduled a software update.

Product information

Provides information on the product name, version, service packs and hotfixes.

Table 3-7 Option definitions

Option	Definition
Product Name	Specifies McAfee Security for Microsoft SharePoint as the product name.
Product Version	Specifies the product version in the format: <Major Version>.<Minor Version>.<build number>.<package number>. For example - 3.0.1000.100
Service Pack	Lists the Service Pack or Patch details (if any).
Hotfixes	Lists the hotfixes and patch installed.

Licenses

Provides information on the type of license, expiration date, and days to expire of the installed product and components.

Table 3-8 Option definitions

Option	Definition
Description	Specifies the installed product name.
Type	Specifies if the installed product is a **Licensed** or **Evaluation** version.
Expires	Appears when you have an **Evaluation** version of the software installed. Specifies the date and time on when the license expires.
Days to Expiry	Appears when you have an **Evaluation** version of the software installed. Specifies the number of days remaining for product expiry. To upgrade an evaluation version of the product to licensed version, contact McAfee support.

View recently scanned items

Provides a quick view of the recently scanned items from the dashboard.

The **Recently Scanned Items** section provides you run-time information on all items scanned by the product. By default, only 10 items appear in the **Recently Scanned Items** section. However, you can view up to 100 items by modifying the **Maximum recently scanned items** option under **Settings & Diagnostics** | **User Interface Preferences** | **Dashboard Settings** | **Report Settings**.

The items in the **Recently Scanned Items** section will be cleared, if you restart **McAfee Portalshield** service from the **Services** console.

Table 3-9 Option definitions

Option	Definition
Date/Time	Date and time when the most recent scan was executed.
Filename	Name of the scanned file.
Detection Name	The name of the detection. For example, the name of a virus.
Folder	Location of the scanned folder in sharepoint.
Username	The name of the user who handled the file.
Direction	The direction of the task. For example, Upload or download.
Action Taken	What action was taken on scanned items.
Scanned By	The policy setting used to scan items. For example On-Demand or On-Access.
Task Name	The name of the task that triggered a detection. For example On-Access scan.
Policy Name	The name of the policy that triggered a detection.

The values **Username**, **Direction**, **Action Taken** and **Scanned By** are available only if you are using SharePoint version 2010 and later.

— Indicates that the item is clean.

— Indicates that the item triggered one of the scanners or filters.

Hover the cursor on to see which scanner or filter was triggered. If the item triggered multiple scanners or filters, only the highest priority detection is shown.

On-Demand scan

An on-demand scanner is a security scanner that you start manually at convenient times or regular intervals. It allows you to set various configurations and scan specific folders.

The software enables you to create scheduled on-demand scans. You can create multiple schedules, each running automatically at predetermined intervals or times.

When should you perform an on-demand scan

- An on-demand scan is highly recommended if there is an outage in your organization due to malicious activity. This will make sure that the Microsoft SharePoint databases are clean and are not infected during the outage.
- McAfee recommends that you perform an on-demand scan task during non-business hours. When an on-demand scan task is scheduled during a non-business hour and it continues during peak work hours, you must reconsider the databases being scanned and create with alternate schedules by altering the data being scanned.
- You can schedule an on-demand scan during the weekends to make sure that the SharePoint databases are clean and older files and folders are also scanned by the latest anti-virus signatures.

Why should you perform an on-demand scan

Perform an on demand scan to:

- Check a specific file or files that are uploaded or published.
- Check that the folders within your SharePoint server are virus-free, possibly following a DAT update, so that new viruses can be detected.
- Check that your computer is completely clean after you have detected and cleaned a virus.
- Check the files and folders which were on your SharePoint server, before you installed McAfee Security for Microsoft SharePoint.
- Check the files and folders which you have not included in on-access scan.

Why should you perform an incremental and resumable scan

After installing McAfee Security for Microsoft SharePoint, run a complete on-demand scan for the first time. Later you can use the incremental scan to scan only the new or modified items on your SharePoint server rather than re-scanning the entire server.

In case of a larger database or server, use resumable scanning. In resumable on-demand scan, if a scan in progress is stopped, McAfee Security for Microsoft SharePoint saves the current state of the scan task. When the same task is started later, scan will resume from the last scanned folder. In the event of a signature (DAT) update while a scan is paused, the software provides an option to restart the scan with the updated DATs.

Best practices for configuring an on-demand policy

- Always enable the anti-virus scanner, DLP and Compliance, and file filtering scanners for on-demand policy. For true file type detection in file filtering, enable DLP and Compliance.
- Select the **High Protection** option to maximize the protection level of the anti-virus scanner.
- Select the **Quarantine** option always so that you can retrieve the files from the quarantine database later if required.
- If SharePoint database size is in GB, make sure to distribute your SharePoint repository (web applications, site collections, sites, folders) in multiple on demand tasks for better performance.
- If McAfee Security for Microsoft SharePoint is installed in a SharePoint Farm setup, distribute your repository on multiple nodes.

For example, in a Farm if you have 4 web applications in your SharePoint server and 4 nodes where the product is installed, you can distribute on demand task in these 4 product nodes.

- McAfee Security for Microsoft SharePoint installation 1 can have on-demand task created for web application 1.
- McAfee Security for Microsoft SharePoint installation 2 can have on-demand task created for web application 2.
- McAfee Security for Microsoft SharePoint installation 3 can have on-demand task created for web application 3.
- McAfee Security for Microsoft SharePoint installation 4 can have on-demand task created for web application 4.

In a SharePoint Farm, every McAfee Security for Microsoft SharePoint **On Demand** displays the whole SharePoint repository.

- Make sure to exclude the SharePoint specific file extension while configuring on demand task. By default these file extensions are not included in the on-demand scan.

Viewing On-demand scan tasks

View a list of on-demand scan tasks configured for McAfee Security for Microsoft SharePoint.

View the on-demand scan tasks from **Dashboard** | **On-Demand Scans**.

Table 3-10 Option definitions

Option	Definition
Name	Indicates the name of the on-demand scan task.
Status	Indicates the current status of the on-demand scan task. The status can be • **Idle** • **Running** • **Stopped** • **Completed**
Last Run	Indicates the date and time, when the on-demand scan was last executed.
Next Run	Indicates the date and time, when the next on-demand scan is scheduled to run.
Action	Lists these options for all the available on-demand scan tasks: • **Modify** • **Delete** • **Run Now** • **Show Status** • **Stop** The **Stop** option appears only if any on-demand scan task is running.
Modify	Edit the settings of an on-demand scan task.
Delete	Deletes the selected on-demand scan task.
Run Now	Starts the selected on-demand scan task immediately.

Table 3-10 Option definitions *(continued)*

Option	Definition
Show Status	Displays the current status of an on-demand scan task. The **Task Status** page appears with these tabs: • **General** — Provides more information on the on-demand scan task such as the total running time of the task, progress of the task, DAT and Engine version used for scanning, scan results, total items scanned, rules broken and folders scanned. • **Settings** — Provides more information on the database scanned and the policy used. • **Detections**— Provides information on the detections triggered during the scan. The **Show Status** option is available only after an on-demand scan task is started.
Stop	Stops an on-demand scan task that is running.
Refresh	Refresh the page with latest on-demand scan information.
New Scan	Schedule a new on-demand scan task. For more information on how to create a new scan, see *Create On-Demand Scan task* section.

Create an on-demand scan task

Schedule an on-demand scan task to find or remove viruses and banned content in files and folders.

Task

1 Click **Dashboard** | **On-Demand Scans**. The **On-Demand Scans** page appears.

2 Click **New Scan**. The **Schedule an on-demand scan** page appears.

3 From **Choose a time** tab, specify when you want the scan to run. The available options are:

- **Not scheduled** — Select this if you have not decided on when to perform the on-demand scan or disable the schedule for an existing on-demand scan.
- **Once** — Specify the date and time to schedule an on-demand scan once.
- **Hours** — Select this to schedule the task based on hours, if you have to execute the on-demand scan task for more than once in a day. For example, let's consider that the current time is 14:00 hours and you have to create a on-demand scan task that satisfies these conditions:
  - The on-demand scan must start exactly at 14:30 hours
  - The on-demand scan must occur twice a day

  To achieve this, specify `12` for hours and `30` for minutes.
- **Days** — Select this to schedule the task based on how often the scan must occur in a week. For example, if you want the on-demand scan to occur once in three days, specify `3` under **day(s)** and select the time when the task should start.

- **Weeks** — Select this to schedule the task based on how often the scan must occur in a month. For example, if you want the on-demand scan to occur bi-weekly, specify `2` under **week(s)**, select the days and time when the task should start.
- **Months** — Select this to schedule the task based on how often the scan must occur in a year. For example, if you want the on-demand scan to occur on every second Saturday of each month, select **second** from **On the** drop-down list, **Saturday** from **of** drop-down list, then select all the months and time when the task should start.

Enable **Stop task after it has run for** <n> **hour(s)** <n> **minute(s)**, to stop an on-demand scan task if it exceeds the specified hours.

4 Click **Next**. The **Choose what to scan** page appears. The available options are:

- **Scan all folders** — Select this to scan all the folders in the SharePoint server.
- **Scan selected folders** — Select this to scan only specific folders in the SharePoint server.
- **Scan all except selected folders** — Select this to scan all except specific folders that are added to the **Folders to scan** list.

Deselect **Scan only document library** to scan all lists in your selected folders.

5 Click **Next**. The **Schedule an on-demand scan** page appears.

6 On the **Excluded file extension(s)**: tab, Specify any file extensions you want to exclude from your on-demand scan in **Specify the file extension(s) separated by ';'** .

By default the extensions `thmx; aspx; asmx; css; jpg; gif; htm; html; png; master; dwp; webpart; bmp` are excluded from the scan. If you want to scan these files, then remove the needed extensions from this list.

7 On the **Advanced**: tab, specify the scan type.

- Select **Off** when you do not want to configure **Resumable Scanning** or **Incremental Scanning**.
- Select **Resumable Scanning** to enable the option to resume on-demand scan from where it stopped, then select **Restart scan if DAT changed** to restart a scan if there is a change in DAT file. For example, if the on-demand scan stops after a specific time, resuming the scan will start the on-demand scan task from the folder where it scanned the last item.
- Select **Incremental Scanning** to scan only the newly added files instead of the whole repository. Select any of the two options for incremental scanning

Option	Definition
Scan from last scanned date	Select this to scan the newly added files from the last scanned date. For the first time, all the files are scanned from the selected target. From the next time, all files where last modified is greater then the last finished time of this task will get scanned.
Scan from date specified	Select this to specify a date and time from which the scan has to start. Default value is today's date and time.

8 Click **Next**. The **Enter a name**: page appears.

9 Specify a meaningful on-demand scan task name, based on the policy you selected in the previous page. For example, if you are creating an on-demand scan task to do a full scan over the weekend, specify the task name as `Weekend Full Scan`.

10 Click **Finish**, then **Apply**.

By performing these steps, you have successfully created an on-demand scan task.

Graphical reports

Generate graphical reports to understand the threat-level during a specific time-frame. Provides an explicit view of detected items in the form of a **Bar Graph** or **Pie Chart**.

These reports help you and your organization to identify servers facing threats.

Use graphical reports when you want to only view the current threat-level and doesn't have to take any action on the detected items. **Graphical Reports** allow you to query based on certain filters, where you can view **Top 10** reports for various detections.

Graphical Reports are classified into:

- **Simple** — Search options to view Top 10 reports of the day or week.
- **Advanced** — More search options to query on different filters, time-range, and chart options.

View graphical reports using simple search filters

Generate graphical report on detections using simple search filters for the day or week.

Task

For option definitions, click **?** in the interface.

1 Click **Dashboard** | **Graphical Reports**. The **Graphical Reports** page appears.

2 Click the **Simple** tab.

3 From **Time Span** drop-down list, select **Today** or **This week** to view detections quarantined for the day or for the week.

4 From **Filter** drop-down list, select the report that you want to view. The options available are:

- **Top 10 Viruses** — Lists the top 10 virus names ranked by their detection count.
- **Top 10 Unwanted Programs**— Lists the top 10 unwanted programs detected that might be threats.
- **Top 10 Unwanted Content Detections** — Lists the top 10 content detections that might be password protected files or signed content.
- **Top 10 DLP and Compliance Detections** — Lists the top 10 data loss prevention and compliance regulatory violations ranked by the number of detections that triggered the rule.
- **Top 10 Infected Files** — Lists the top 10 filenames ranked by their detection count.
- **Top 10 Detections** — Lists the top 10 detections ranked by their detection count. This graph contains all the categories such as viruses, Unwanted programs, DLP and compliance, and infected files listed above.
- **Top 10 Virus Senders** — Lists the top 10 user names ranked by their virus detection count.
- **Top 10 Unwanted Content Senders** — Lists the top 10 user names ranked by their content detection.
- **Top 10 Virus Upload Locations** — Lists the top 10 folder locations ranked by their virus detection count.
- **Top 10 Virus Unwanted Content Locations**— Lists the top 10 folder locations ranked by their content detection.

- **Top 10 Virus DLP and Compliance Senders**— Lists the top 10 user names ranked by the number of detections that triggered the DLP and Compliance rules.
- **Top 10 Virus DLP and Compliance Locations**— Lists the top 10 folder locations ranked by the number of detections that triggered the DLP and Compliance rules.
- **Top 10 File Filter Detections**— Lists the top 10 file filter detections triggered by the system.
- **Top 10 File Filter Senders**— Lists the top 10 user names ranked by their file filter detections.
- **Top 10 File Filter Locations**— Lists the top 10 folder locations ranked by their file filter detections.

5 Click **Search**. The search results are shown in the **View Results** pane.

In **Magnify Graph**, select the zoom percentage to let you enlarge or reduce the view of the graph in the **View Results** pane.

View graphical reports using advanced search filters

Generate graphical report on detections using advanced search filters.

Task

For option definitions, click **?** in the interface.

1 Click **Dashboard** | **Graphical Reports**. The Graphical Reports page appears.

2 Click **Advanced** tab.

3 Select at least one filter or up to three filters from the list:

Table 3-11 Primary Filters

Filter	Description
Reason	Search using the detection trigger or using the reason why the item was quarantined. When you select the **Reason** filter, secondary filters are enabled for further refining your search. For example, you might want to search for all items that was quarantined due to the **File Filter** rule being triggered as the reason.
Ticket Number	To search using the ticket number. A ticket number is a 16-digit alpha-numeric entry that is auto-generated by the software for every detection.
Detection Name	To search by the name of a detected item.
Scanned by	To search by the type of the scan. For example On-Demand or On-Access.
The below listed features are available if you are using Microsoft SharePoint 2010 and later.	
Username	To search by the name of the user whose file triggered the detection.
Direction	To search by the access mode of the file. For example Upload or Download.
Folder	To search by the SharePoint folder of the files that were quarantined.
RMS Protection	Search for files that are listed as RMS Protected. Rights Management Service is Microsoft service by which the users can prevent unauthorized access to documents. If you have RMS server set up to protect your documents, then they will be shown under RMS Protection.

A secondary filter is available for the **Reason**, **Scanned by** and **Direction** filters. If you do not want specify the secondary filter, ensure that the field is blank so that all detections are queried upon.

Table 3-12 Secondary filters for Reason

Filter	Description
Anti-Virus	Search for items that were detected when a potential virus was found in files.
DLP and Compliance	Search for items that were detected when a non compliant file was uploaded.
File Filter	Search for items that were detected when a banned file extension was uploaded.
Encrypted or Corrupted	Search for items that were detected when encrypted or corrupt content was found in files.
Potentially Unwanted Program	Search for items that were detected when potentially unwanted program was found in files.
Packer	Search for items that were detected when packers (small programs, compressed executables files, encrypted code) was found in files.
Encrypted	Search for items that were detected when encrypted content was found in files.
Signed	Search for items that were detected when signed content was found in files.
Corrupted	Search for items that were detected when corrupt content was found in files.
Denial of Service	Search for items that were detected when denial-of-service threat occurred.

Table 3-12 Secondary filters for Reason *(continued)*

Filter	Description
Protected Content	Search for items that were detected when protected content was found and the content might not be accessed for scrutiny.
Password Protected	Search for items that were detected when password protected content was found and the content might not be accessed for scrutiny.
On Scan Failure	Search for items that could not be scanned.

Table 3-13 Secondary filters for Scanned by

Filter	Description
On-Demand	Search for items that were detected by On-Demand scan.
On-Access(WSS VS API)	Search for items that were detected by On-Access scan.

Table 3-14 Secondary filters for Direction

Filter	Description
Upload	Search for items that triggered the detection when items are uploaded to the SharePoint server.
Download	Search for items that triggered the detection when items are downloaded from the SharePoint server.

4 Select **All Dates** or a **Date Range** from the drop-down lists.

If you select **All Dates**, the query returns search results from quarantine database from day it started quarantining any detected items. If you select **Date Range**, select the **Date**, **Month**, **Year**, **Hour**, and **Minutes** from the **From** and **To** fields to enable your query to search within a date range.

5 Select **Bar Graph** or **Pie Chart** as required.

6 If you select **Pie Chart**, select a filter from the drop-down list to further refine your search:

Table 3-15 Query on

Filter	Description
Filename	Sort by a quarantined filename.
Detection Name	Sort by the name of a detected item.
Reason	Sort by the detection trigger or using the reason why the item was quarantined.
Rule Name	Sort by the name of the rule that triggered the detection.
Policy Name	Sort by the policy name that triggered the detection.
Scanned by	Sort by the name of the scan.
Username	Sort by the name of the user whose files triggered the detection.
Direction	Sort by the direction of the file.
Folder	Sort by the folder of the files that were quarantined

a In **Maximum Results**, specify the number of search results you want to view. You can view a maximum of 99 search results and this field is available only if you select pie chart.

7 Click **Search**. The search results are shown in the **View Results** pane. In **Magnify Graph**, select the zoom percentage to let you enlarge or reduce the view of the graph in the **View Results** pane The search results are shown in the **View Results** pane.

You have now generated graphical reports of detections.

4 Detected items

View information about all items containing potential threats that are detected and quarantined by McAfee Security for Microsoft SharePoint. You can use various search filters to refine the search and find quarantined items that are of interest to you, view the results and take necessary action on the quarantined items.

Contents

- *Primary search filters*
- *Additional search options*
- *Search detected items*
- *Actions that you can take on quarantined items*

Primary search filters

Search filters enable you to define the search criteria and provide more efficient and effective searches from the quarantine database.

These search filters appear in the **View Results** section of the detected item category.

Use **Columns to display** in the **View Results** section, to select the search filters that you want to view.

Table 4-1 Detected items — Primary search filters

Search filter	Definition
Filename	Search by the name of the detected file in the quarantined item. To view the **File Name** used, go to **Policy Manager** | **Shared Resource** | **DLP and Compliance Dictionaries** | **File Filtering Rules**.
Action taken	Search for an item based on the action that was taken on it. For example**Prevent Upload/ Download of the Item** or **Allow through**
Username	Search for an item by the user whose actions triggered the detection.
Folder	Search by the folder where quarantined items are stored.
Direction	Search by the direction of the file. For example **Upload** or **Download**.
RMS Protection	Search for files which are RMS Protected. Rights Management Service is Microsoft service which prevents unauthorized access to documents. If you have RMS server set up to protect your documents, then they will be shown under RMS Protection.
Detection Name	Search for a detected item based on its name.
Ticket Number	Search for an item based on the ticket number, which is a unique alphanumeric identifier assigned to a specific detection. It helps identify the associated detection.
Scanned By	Search by the name of the scan. For example **On-Demand** or **On-Acess(WSS VS API)**.

Table 4-1 Detected items — Primary search filters *(continued)*

Search filter	Definition
Policy Name	Search for an item by a policy name such as a **Master policy** or sub-policy that detected the item.
Reason	Search for an item based on the reason why it was detected. The reasons are • **Anti-Virus** • **DLP and Compliance** • **File Filter** • **Encrypted or Corrupted** • **Potentially Unwanted Program** • **Packer** • **Encrypted** • **Signed** • **Corrupted** • **Denial of Service** • **Protected Content** • **Password Protected** • **On Scan Failure**

Additional search options

Provides information on additional search options to narrow-down the detected items search results.

Table 4-2 Option definitions

Option	Definition
All Dates	Select if you want to search for items on all dates. The search results appear based on the date stored in the quarantined items database.
Date Range	Search for an item within a defined date range according to your requirements. Here you can specify the date, month, year and time against the parameters **From** and **To**. You can also use the calendar icon to specify a date range. The date range is based on the local system time.
Search	Click to view a list of quarantined items matching your search criteria that appear in the **View Results** section.
Clear Filter	Click to return to default search settings.

Search detected items

Use search filters to find specific quarantined items that are of interest to you and take corresponding action.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Detected Items**.

2 From the left-pane, click the desired detection category such as **Viruses**, **Potentially Unwanted Programs**, **Banned File types/Messages**, **DLP and Compliance**, **Unwanted Content** or **All Items**.

3 From the **Search** pane, select the desired search filters from the drop-down lists (if required). The available search options are:

Table 4-3 Search options

Search feature	Description
Primary search filter	Select if you want to refine your search criteria based on a specific filter such as **Policy Name**, **Action Taken**, **Sender** and so on. For more information on all primary search filters, see *Available primary search options* section.
Date Range	Select if you want to refine your search to all dates or to a specific time frame. • **All Dates** • **Date Range**

4 Click **Search**.

By performing this task, you have successfully searched for detected items matching your search criteria, that now appear in the **View Results** section.

To specify a limit on how many quarantined items need to appear in the **View Results**, modify the **Maximum query size (records)** value from **Settings & Diagnostics** | **Detected Items** | **Local Database**.

Actions that you can take on quarantined items

View results of the search based on the parameters you defined and take necessary action on quarantined items.

You can then execute these actions on quarantined items.

Table 4-4 Types of action

Action	Definition
Download	To download a quarantined item for research or analysis. Select one applicable record from the **View Results** pane and click **Download**. You cannot **Download** multiple records at a time.
Export to CSV File	To export and save information about all quarantined items returned by the search in a `.CSV` format. If there are thousands of quarantined items in the database, instead of navigating through multiple pages, you can use this option to download these records to a file in CSV format and later generate custom reports in Microsoft Excel. From the **View Results** pane, click **Export to CSV File** to **Open** or **Save** the search results to the desired folder or location. • If you do not find a specific field in the search result of the CSV file, make sure to enable the required field in the **Columns to Display** option. • Use the **Import Data** option in Microsoft Excel, to open the CSV file in a different locale.
Columns to display	To select additional column headers to be listed in the **View Results** pane. This option has a list of all the filters available in the **Search** pane and some more options.

Table 4-4 Types of action *(continued)*

Action	Definition
Select All	To select all quarantined items that appear in that page of the **View Results** section. For example, if you have 100 quarantined items and set the items to view **per page** as 10, then only 10 items that appear in the **View Results** section is selected.
Select None	To deselect all quarantined items that appear in the **View Results** section.
Delete	To delete the quarantined items that you selected in that page of the **View Results** section for the selected category. Press and hold down the **Ctrl** key to select multiple items.
Delete All	To delete all quarantined items from the database for the selected category.
Views **per page**	To specify the maximum number of quarantined items that you want to view per page. The options are: • **10** • **20** • **50** • **100**

Each item in the **View Results** pane has an image, which indicates:

Icon	Description
	An item that is quarantined and can be downloaded.
	An item that is only logged and cannot be downloaded.

5 Policy Manager

You can configure or manage different policies and corresponding actions in the product.

A policy is typically described as a principle or rule to guide decisions and achieve rational outcomes. Policies are adopted within an organization to help objective decision making.

In McAfee Security for Microsoft SharePoint, a policy specifies the settings that are used and the actions to take when a detection is triggered. You can create multiple policies and define specific settings and actions to the particular policies. For example, you can create multiple sub-policies for the **On-Access** menu option and have a different setting and action set for each policy.

Use the **Shared Resource** menu option under **Policy Manager**, to modify or create rules for scanner, filter, and alert settings from one common location. Use **Shared Resource** to save time in creating and applying the policies.

Contents

- *Policy manager menu options*
- *Policy categories to handle threats*
- *Policy manager views*
- *Master policy and sub-policy*
- *Core scanners and filters*
- *List all scanners and filters for a selected policy*
- *Add a scanner or filter*
- *Create policy rules*
- *Actions you can take on detections*
- *Shared resource*
- *Manage core scanner settings for a policy*
- *Manage filter settings for a policy*

Policy manager menu options

View the menu options available under **Policy Manager**.

From the product's user interface, click **Policy Manager**. These menu options appear on the navigation pane.

Option	Description
On-Access	Contains policies for files and documents every time they are uploaded or downloaded, to determine if it contains a virus or other threats.
On-Demand	Contains policies that are activated at set intervals or on demand, to find a virus or other threats.
Shared Resource	One common location to edit settings for scanners, filters, alerts, DLP and Compliance dictionaries, and time slots.

Policy categories to handle threats

View available policy categories and apply an existing default policy (known as a *Master Policy*) to your entire organization.

The software helps you mitigate electronic threats with special set of rules and settings called policies, that you can create to suit your organization needs.

When you install the software, for the first time on your server, a default **Master policy** is available for these menu options:

- **On-Access**
- **On-Demand**

You can customize policies under on-access or on-demand to precisely handle specific threats that could affect your SharePoint server.

Policy manager views

View and sort sub-policies based on inheritance or priority.

The types of **Policy Manager** views are:

- **Inheritance View**
- **Advanced View**

Inheritance view

Displays the priority and status of the Master policy and all sub-policies. The software acts on an item, based on the settings configured for the sub-policy with highest priority. When the rules of a sub-policy are not satisfied, the sub-policy with the next priority is considered. Settings configured in the Master policy are applied, when rules in none of the sub-policies are satisfied.

When you select **Inheritance View**, the sub-policies appear based on the inheritance of the policy.

In this view, you can:

- View the policy and its priority
- View the inherited sub-policy and its parent policy
- Enable or disable sub-policies
- Delete sub-policies

Advanced view

Display all policies in ascending order, based on the priority and provides an option to change the priority of a sub-policy.

In this view, you can:

- View the policies sorted on priority
- Modify the priority of a policy

Use these icons to modify the priority of a policy:

- — Increase the priority of a sub-policy.
- — Decrease the priority of a sub-policy.

- Enable or disable sub-policies
- Delete sub-policies
- Edit the policy name, description, and parent policy by clicking **Details**

Master policy and sub-policy

A policy setting inside a hierarchical structure is ordinarily passed from parent to children, and from children to grandchildren, and so forth. This concept is termed as inheritance. The default parent policy is referred as **Master policy** and child policy is referred as **Sub-policy**.

Master policy

Default parent policy available for all policy categories that defines how items are scanned for viruses, how files are filtered, and various other settings.

You cannot delete the **Master policy**, as it acts as a baseline to create sub-policies.

Sub-policy

A policy which inherits settings and actions from another policy is known as sub-policy.

Sub-policies are required in situations where you need exceptions to the **Master policy** to suit any geographical areas, functions, domains, or departments within your organization.

Action taken on an item is based on the settings configured for the sub-policy with highest priority. When the rules of a sub-policy with highest priority are not satisfied, the software moves on to the sub-policy with the next priority. Settings configured in the Master policy are applied only when rules in none of the sub-policies are satisfied.

If you select **Inherit settings from parent policy** in the scanner or filter settings page, an inherited policy (sub-policy) uses the same setting as the parent policy. However, if there is a detection, you can take a different action. Any changes to the settings in the parent or **Master policy** is reflected in these sub-policies.

Restoring the software to default setting removes the existing sub-policies. Make sure to back up the policies and settings using **Export** from **Settings & Diagnostics** | **Import and Export Configuration** | **Configuration** tab, before restoring the product to factory settings.

Create sub-policies

Create other policies based on the **Master policy** or a parent policy to suit specific needs of any part of your organization. Create sub-policies for any exceptional situations that are not covered by the **Master policy**.

This is useful when you do not want to apply rules from the **Master policy** for certain types of files in your organization. You can create exceptions and allow the software to perform specific scan.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface click **Policy Manager**, select a menu item for which you want to create a sub-policy.

2 Click **Create Sub-policy**.

The **Create a sub-policy** page appears.

3 Under **Initial configuration** | **Identification** | **Sub-policy name**, specify a name that identifies the policy and what it does.

4 Type a **Description** for the policy (optional).

5 Select the **Parent policy** for the sub-policy from where to inherit the settings.

6 Click **Next**.

7 Under **Trigger Rules** | **Specify policy rules**, click **New Rule** to create a new rule.

Specify a policy rule page appears.

8 From **Specify a policy rule**, you can select:

- **<select a rule template>** — To specify a policy rule based on the file name. You can create new rules, based on these options:
  - **The file name is file name**
  - **The file name is not file name**
- **Copy rules from another policy** — To copy the rules from another policy.

9 Specify the conditions when the policy should trigger for the user. You can select:

- **Any of the rules apply**— Specify if any of the rules created is applied to the policy.
- **All rules apply**— Specify if all the rules created are applied to the policy.
- **None of the rules apply —** Specify if none of the rules created are applied to the policy.

10 Click **Add**.

To delete a rule, select a rule and click on **Delete**.

11 Click **Next**.

12 From **Scanner and Filters**, you can select:

- **Inherit all settings from the parent policy** — To inherit all properties of the parent policy.
- **Initialize selected settings with values copied from another policy** — To select specific scanners and filters from the available policies. You can select and deselect any of the scanners and filters.

13 Click **Finish**.

You have now created a sub policy.

Core scanners and filters

Determine the types of scanners and filters that can be applied when creating policies.

Core scanners

View and configure settings for these scanners from **Policy Manager** | **On-Access**.

Scanner	Definition
Anti-Virus Scanner	Configure settings to detect threats such as viruses, trojans, worms, packers, spyware, adware, and more.
DLP and Compliance Scanner	Create or configure **DLP and Compliance Rules** to meet your organization's confidential and compliance policies with the addition of 60 new **DLP and Compliance Dictionaries**.
File Filtering	Create new file filtering rules to meet the organization needs. Configure these settings to detect files based on file name, file category, or file size.

Filters

Specify actions to take when there is a detection, based on your organization needs.

Filter	Definition
Corrupt Content	Configure settings to act on items that are detected as corrupt content.
Protected Content	Configure settings to act on items that are detected as protected content.
Encrypted Content	Configure settings to act on items that are detected as encrypted content.
Signed Content	Configure settings to act on items that are detected as signed content.
Password-Protected Files	Configure settings to act on items that contain password protected files.
Scanner Control	Create or configure core scanner settings to act on items based on the nesting level, expanded file size, and scanning time.

List all scanners and filters for a selected policy

View status of the available scanners and filters for the selected policy category.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Policy Manager** and policy category menu item.

The policy page for the selected menu item appears.

2 Click **Master policy** or the required sub-policy.

The corresponding policy page appears.

3 In the policies page, you can use these tabs:

- **List All Scanners** — To view which scanner or filter is enabled for the policy.
- **View Settings** — To view settings of the scanner or filter and the actions specified.
- **Specify Rules** — To specify policy rules that apply to specific type of items or files.

  You can specify policy rules only to sub-policies.

4 From the **List All Scanners** tab, you can use:

Table 5-1 Policy configuration

Option	Definition
Policy	To select the policy, you want to configure.
Add Scanner/Filter	To configure the policy so that it applies only at specific times. For example, you can create new anti-virus setting with different rules, which is applicable only on weekends.
Core Scanners	To configure the policy for each of these scanners: • **Anti-Virus Scanner** • **DLP and Compliance Scanner** • **File Filtering**
Filters	To configure the policy for each of these filters: • **Corrupt Content** • **Protected Content** • **Encrypted Content** • **Signed Content** • **Password Protected Files** • **Scanner Control**
Inherits	This specifies if the core scanners and filters are inherited from the master policy. • ✔ indicates that the scanner or filter is inherited. • This is not applicable for master policy.

Add a scanner or filter

Add a scanner or filter to create settings for exceptional scenarios in your organization.

Adding a scanner or filter is useful, when you want an additional scanner or filter:

- With different options and rules
- To enable them only during a specific time slot

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a policy category.

2 Click **Master Policy** or any sub-policy.

3 From the **List All Scanners** tab, click **Add Scanner/Filter**.

4 From **Specify the category** drop-down list, select the required scanner or filter.

5 From **When to use this instance** section, select an existing time slot or create a new one.

- **Select existing time slot**— Specify a time slot which already exists.
- **Create a new time slot** — Create a new time slot. Specify the options:

Option	Definition
Time slot name	Specify the name of the time slot such as weekends, weekdays.
Select day and time	Select the desired day of the week.
All day	Select to specify the entire day.
Selected hours	Select to specify the start and end time.

6 Click **Save**.

7 Click **Apply**.

Edit the options and rules to suit your organization needs.

Create policy rules

Build new rules and specify conditions for a policy.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a policy category.

2 Click **Master policy** or a sub-policy.

3 Click the **Specify Rules** tab.

4 Click **New Rule**.

5 From **Specify a policy rule**, you can select:

- **<select a rule template>** — To specify a policy rule based on the file name. You can create new rules, based on these options:
  - **The file name is file name**
  - **The file name is not file name**
- **Copy rules from another policy** — To copy the rules from another policy.

6 Click **Add**.

7 To delete a rule, select a rule and click **Delete**.

8 Specify the conditions when the policy should trigger. You can select:

- **Any of the rules apply** — Specify if any of the rules created is applied to the policy.
- **All rules apply** — Specify if all the rules created are applied to the policy.
- **None of the rules apply** — Specify if none of the rules created are applied to the policy.

9 Click **Apply** to save the rule.

Actions you can take on detections

For each scanner and filter settings in a policy, you can specify a primary and secondary action to take on a detection. You can specify what happens to an item, when it triggers a detection.

When a policy rule is triggered based on the scanner or filter settings, the software acts on the detection based on the primary and secondary action configured.

When configuring actions, at least one primary action must be selected. You can also select a number of secondary actions. For example, if the primary action is preventing upload/download of an item that triggers a detection, the secondary action might be logging the detection and quarantining it.

The available primary actions depend on the type of policy category and scanner or filter settings you configure.

Click **Reset**, to restore the actions to default settings for the policy category and scanner.

Table 5-2 Primary actions

Action	Definition
Attempt to clean any detected virus or trojan	To clean an item from a virus or trojan detected by the **Anti-Virus Scanner**.
Replace item with an alert	To replace an item that triggered the detection with an alert.
Remove embedded item	To replace an attachment that triggered the detection in a document.
Prevent Upload/Download of the Item	To prevent upload or download of an item that triggered a detection.
Allow through	To allow the item to reach the next phase.

Table 5-3 Secondary actions

Action	Definition
Log to Detected Items	To record the detection in a log.
Quarantine	To store a copy of the item that triggered the detection in the quarantine database. To view all quarantined items, go to **Detected Items** | **All Items** or the specific detection category.

Shared resource

One common location to edit settings for scanners, filters, alerts, DLP and Compliance dictionaries, and time slots. When setting up policies, you might want the same resource (scanner and filter settings) applied to more than one policy. In such scenarios, use **Shared Resource**.

From the product's user interface, click **Policy Manager** | **Shared Resource**. You can use these tabs:

- **Scanners & Alerts** — To edit or create new scanner and filter settings.
- **DLP and Compliance Dictionaries** — To edit or create new **DLP and Compliance Rules** and **File Filtering Rules**.
- **Time Slots** — To edit or create new time slots such as weekdays or weekends.

Any changes made to these settings are applied automatically to all policies using these configurations.

Configure scanner settings

Create or modify scanner settings to suit your organization's requirement.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Policy Manager** | **Shared Resource**.

The **Shared Resources** page appears.

2 Click **Scanners & Alerts** tab.

3 From the **Category** drop-down list under **Scanners** section, select the scanner you want to configure. The scanner type appears with the settings name, policies used by, and action to configure. You can use:

Table 5-4 Option definitions

Option	Definition
Category	To select the required scanner that you want to configure.
Create New	To create new settings for a scanner based on your requirement. Required in a situation where you need exceptions for certain scanner settings and apply it in a policy.
Edit	To edit settings for the selected scanner.
Delete	To delete the scanner settings. You cannot delete a scanner, if it is a default scanner and if it is used by any policy. To see how many policies use this scanner setting, see the **Used By** column.

4 Once you configure the scanner settings, click **Save**, then **Apply**.

Configure alert settings

Create or modify alert settings for the selected scanner to suit your organization's requirement.

Alert settings are applicable only for on-demand policies.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Policy Manager** | **Shared Resource**.

The **Shared Resources** page appears.

2 Click **Scanners & Alerts** tab.

3 From the **Category** drop-down list under **Alerts** section, select the alert you want to configure for a scanner. The scanner type appears with the settings name, policies used by, and action to configure. You can use:

Table 5-5 Option definitions

Option	Definition
Category	To select the required scanner that you want to configure.
Create New	To create new settings for a scanner based on your requirement. Required in a situation where you need exceptions for certain scanner settings and apply it in a policy.
View	To view the default alert settings for a scanner.
Edit	To edit settings for the selected scanner.
Delete	To delete the scanner settings. You cannot delete an alert, if it is a default scanner alert and if it is used by any policy. To see how many policies use this alert setting, see the **Used By** column.

4 Once you configure the scanner settings, click **Save**, then **Apply**.

You have now successfully configured the settings for an alert, based on your organization's requirement.

Create a new alert

Create a new alert message for actions taken by a scanner or filter.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Policy Manager** | **Shared Resource**.

The **Shared Resources** page appears.

2 Click **Scanners & Alerts** tab.

3 From the **Category** drop-down list under **Alerts** section, select the alert you want to configure for a scanner.

4 Click **Create New**.

The **Alert Editor** page appears.

5 Type a meaningful **Alert name**.

6 Select the required **Style**, **Font** and **Size** from the respective drop-down lists.

These options are available only if you select **HTML content (WYSIWYG)** from the **Show** drop-down menu.

7 Select the values you want to include in your alert message from **Tokens** drop-down list.

- **DETECTIONS** — The list of detections in the item.
- **ATTACHMENTNAME** — The name of the item being scanned.
- **ACTIONNAME** — The actions taken on the detected item.
- **AVDATVERSION** — The DAT verison used by the anti-virus engine

- **AVENGINEVERSION** — The version of the anti-virus engine.
- **TICKETNUMBER** — The 16-digit alpha-numeric entry which is auto-generated by the software for every detection.

8 Use any of these tools to customize your alert:

Table 5-6 Toolbar options

Options	Description
Bold	To make the selected text bold.
Italic	To make the selected text italic.
Underline	To underline the selected text.
Align Left	To left align the selected paragraph.
Center	To center the selected paragraph.
Align Right	To right align the selected paragraph.
Justify	To adjust the selected paragraph so that the lines within the paragraph fill a given width, with straight left and right edges.
Ordered List	To make the selected text into a numbered list.
Unordered List	To make the selected text into a bulleted list.
Outdent	To move the selected text a set distance to the right.
Indent	To move the selected text a set distance to the left.
Text Color	To change the color of the selected text.
Background Color	To change the background color of the selected text.
Horizontal Rule	To insert a horizontal line.
Insert Link	To insert a hyperlink where the cursor is currently positioned. In **URL**, type the **URL**. In **Text**, type the name of the hyperlink as you want it to appear in the alert message. If you want the link to open a new window, select **Open link** in new window, then click **Insert Link**.
Insert Image	To insert an image where the cursor is currently positioned. In **Image URL**, type the location of the image. In **Alternative text**, type the text you want to use in place of the image when images are suppressed or the alert message is displayed in a text-only browser. If you want to give the image a title, type the title name in **Use this text as the image title**. Click **Insert Image**.
Insert Table	To insert a table at the current cursor position. Type the values in **Rows**, **Columns**, **Table width**, **Border thickness**, **Cell padding**, and **Cell spacing** to configure the table, then click **Insert Table**.

9 From the **Show** drop-down menu, specify how the alert message should be displayed within the user interface. You can select:

- **HTML content (WYSIWYG)** — To hide the underlying HTML code and display only the content of the alert message.
- **HTML content (source)** — To display the alert message with the HTML code as it appears before compilation.
- **Plain-text content** — To display the content as plain text.

10 Click **Save** to return to the policy page.

Click **Reset** to undo all changes you have made since you last saved the alert message.

Configure DLP and Compliance rules

Create or modify DLP and Compliance rules and dictionaries, to suit your organization's requirement.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Policy Manager** | **Shared Resource**.

The **Shared Resources** page appears.

2 Click **DLP and Compliance Dictionaries** tab.

3 From the **Category** drop-down list under **DLP and Compliance Rules** section, select the category you want to view or configure. The rules group appears with the name, policies used by, and action to configure. You can use:

Table 5-7 Option definitions

Option	Definition
Category	To select the required scanner that you want to configure. This release has 60 more DLP and Compliance dictionaries ensuring that content is in accordance with your organization's confidentiality and compliance policies. Pre-defined Compliance Dictionaries include: • Addition of 60 new DLP and Compliance dictionaries • Support for industry specific compliance dictionaries - HIPAA, PCI, Source Code (Java, C++ etc.) These dictionaries are categorized as: • Score based — A rule is triggered when the document exceeds the threshold score and maximum term count, resulting in reduced false positives. • Non-score based — A rule is triggered when a word or phrase is found in the document. For information on score based and non score based dictionaries, see *Configure DLP and compliance scanner settings*.
New Category	To create a new **DLP and Compliance Rules** dictionary. Any new category or condition that you create is non-score based.

Table 5-7 Option definitions *(continued)*

Option	Definition
Create New	To create new rules group for the selected category, based on your requirement. Required in a situation where you need specific rules to trigger a detection and apply it in a policy.
Edit	To edit settings for the selected **DLP and Compliance** rule.
Delete	To delete the **DLP and Compliance** rule. You cannot delete a **DLP and Compliance** rule, if • It is enabled. Deselect the rule, **Apply** the settings, then click **Delete**. • If it is used by any policy. To know, how many policies use this scanner setting, see the **Used By** column.

For example, select **Credit Card Number** or any dictionary that suits your needs, from the **Category** drop-down list and see the enhanced **Rules Group** option available.

4 To create a new rules group, click **Create New** for **DLP and Compliance Rules** for a selected category.

The **New DLP and Compliance Scanner Rule** page appears for the selected category.

5 Type the **Rule Name** and **Description** for the rule.

6 Select **Add this rule to this category's rules group** to add the new rule to the rules group for the selected category.

7 Under **Word or Phrase**, specify the words or phrases to look for, in **The rule will trigger when the following word or phrase is found**. Then select one of the following options:

- **Regular Expression** — If enabled, the rule is triggered for specified text that is a regular expression (regex). Regex is a precise and concise method for matching strings of text, such as words, characters, or patterns of characters.

  For example, the sequence of characters "tree" appearing consecutively in any context, such as trees, street, or backstreet.

  Regex is disabled for some phrases. see http://www.regular-expressions.info/reference.html or http://www.zytrax.com/tech/web/regex.htm for details.

- **Use Wildcard** — If enabled, the rule is triggered for the specified word or phrase that contain wildcard characters. (Wildcard characters are often used in place of one or more characters when you do not know what the real character is or you do not want to type the entire name).
- **Starts with** — If enabled, the rule is triggered for specified text that forms the beginning of the word or phrase.
- **Ends with** — If enabled, the rule is triggered for specified text that forms the last part of the word or phrase.
- **Case Sensitive** — If enabled, the rule is triggered if the case of the specified text matches the word or phrase.

  To detect a word or phrase with exact match, select both **Starts with** and **Ends with** option.

8 Select **Specify additional contextual words or phrases**, which is a secondary action when the primary word or phrase is detected. Specify any additional word or phrase that can accompany the primary word or phrase that triggers a detection.

9 Select from **Trigger if ALL of the phrases are present**, **Trigger if ANY of the phrases are present** or **Trigger if NONE of the phrases are present** from the drop-down menu.

10 Select **within a block of** to specify the number of **Characters** from a block to be scanned.

11 Click **Add Contextual word** to type additional words or phrases.

12 Specify the word or phrase in **Specify words or phrases**, select one of the conditions (same options as in Step 7), then click **Add**.

13 Under **File Format**, select **Everything** to enable all file categories and its subcategories. You can select multiple categories and file types within the selected categories to be matched. Selecting **All** in the subcategory selector overrides any other selections that may have already been made.

14 If you have not selected **Everything**, then click **Clear selections** to deselect any of the selected file type options.

15 Click **Save** to return to **Shared Resources** page.

16 Click **Apply** to save the settings.

You have now successfully configured the DLP and Compliance rules and dictionaries, to suit your organization's requirement.

Configure file filtering rules

You can use file filtering rules to monitor and restrict the movement of files. You can filter files according to their file name, category type, and size.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Policy Manager** | **Shared Resource**.

The **Shared Resources** page appears.

2 Click **DLP and Compliance Dictionaries** tab.

3 From **File Filtering Rules**, click **Create New**.

The **File Filtering Rule** page appears.

4 Type a unique **Rule name**. Give the rule a meaningful name, so that you can easily identify it and what it does. For example, FilesOver5MB or Block MPP files.

5 In the **File Filtering Rule** page, you can use:

Table 5-8 Option definitions — Filename filtering

Option	Definition
Enable file name filtering	To enable file filtering according to the file names.
Take action when the file name matches	Specify the name of the files that triggers this rule. You can use wildcard characters (* or ?) to match multiple file names. For example, if you want to filter any Microsoft PowerPoint files, type `*.ppt`.
Add	To add the file name specified under **Take action when the file name matches**, to the file name filtering list.

Table 5-8 Option definitions — Filename filtering *(continued)*

Option	Definition
Edit	To edit or modify an existing file filtering rule.
Delete	To remove the file name from the filtering list. You cannot delete a file filtering rule, if it is used by any policy. The **Used By** column must display **0 policies** for the rule that you want to delete. You must first remove the file filtering rule from the policy, then click **Delete**.

Table 5-9 Option definitions — File category filtering

Option	Definition
Enable file category filtering	To enable file filtering according to their file type.
Take action when the file category is	Specify the type of files that affects this rule. File types are divided into categories and subcategories.
File categories	Select a file type category. An asterisk symbol (*) appears next to the file type, to indicate that the selected file type will be filtered.
Subcategories	Select the subcategory you want to filter. To select more than one subcategory, use **Ctrl**+**Click** or **Shift**+**Click**. To select all of the subcategories, click **All**. Click **Clear selections** to undo the last selection.
Extend this rule to unrecognized file categories	To apply this rule to any other file categories and subcategories that are not specifically mentioned in the categories and subcategories list.

Table 5-10 Option definitions — File size filtering

Option	Definition
Enable file size filtering	To filter files according to their file size.
Take action when the file size is	Specify a value in the adjacent text box and drop-down list, then select: • **Greater than** — To specify that the action should only be applied if the file is larger than the size specified. • **Less than** — To specify that the action should only be applied if the file is smaller than the size specified.

6 Click **Save** to return to the **Shared Resources** page.

7 Click **Apply** to create the file filtering rule.

You have now successfully created a file filtering rule.

Configure time slots

Set up different time slots or configure existing time slots that can be applied to policies, based on your organization's requirement.

Time Slots enable you to specify the time during which certain rules must be triggered. For example, you might want to restrict large file upload or download during office hours.

There might be situations where you require more time slots, based on different users, their geographical locations, or working hours. You can create more time slots based on business hours, non-business hours, weekly maintenance, and so on.

By default, the software has these time slots:

- **All the time**
- **Weekdays**
- **Weekends**
- **Working hours**

You cannot delete or edit the default time slot **All the time**, as the **Master policy** uses it.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Policy Manager** | **Shared Resource**.

The **Shared Resources** page appears.

2 Click **Time Slots** tab.

3 Click **Create New**.

The **Time Slot** page appears.

4 Type a unique **Time slot name** such as `Business hours` or `System Maintenance (Weekly)`.

5 Under **Select day and time**, select the required days.

6 Select **All day** or **Selected hours**.

7 Specify the **Start** and **End** time from the drop-down list, if you choose **Selected hours**.

8 Click **Save** to return to the **Shared Resources** page.

9 Click **Apply** to save the settings.

You have now successfully configured or created a time slot, to suit your organization's requirement.

Manage core scanner settings for a policy

Create or edit scanner options, then specify an appropriate action to take on the detected item when a policy is triggered.

The available core scanners are:

- **Anti-Virus Scanner**
- **DLP and Compliance Scanner**
- **File Filtering**

Tasks

- *Configure anti-virus scanner settings* on page 55
  Configure **Anti-Virus Scanner** settings in a policy to identify, thwart, eliminate computer viruses and other malware.
- *Configure file filtering settings* on page 57
  Configure settings in a policy to detect files based on their name, type, or size and take necessary actions.
- *Configure DLP and Compliance scanner settings* on page 58
  Configure **DLP and Compliance Scanner** settings in a policy to identify noncompliant data in documents or other items and take necessary actions.

Configure anti-virus scanner settings

Configure **Anti-Virus Scanner** settings in a policy to identify, thwart, eliminate computer viruses and other malware.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the anti-virus scanner.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **Anti-Virus Scanner**.

4 In **Activation**, select **Enable** to activate the anti-virus scanner settings for the selected submenu item.

If you are configuring settings for a sub-policy, select **Use configuration from parent policy** to inherit settings from the parent policy.

5 From the **Options** section, you can use:

Table 5-11 Option definitions

Option	Definition
High Protection	To scan all files, archive files, unknown viruses, unknown macro viruses, potentially unwanted programs, and scan all files for macros.
Medium Protection	To scan all files, archive files, unknown viruses, unknown macro viruses, and potentially unwanted programs.
Low Protection	To scan only default file types, archive files, and potentially unwanted programs.
<create new set of options>	To create your customized anti-virus scanner settings.
Edit	To edit the existing level of protection.

6 If you select to edit or modify the scanner settings, in **Instance name**, type a unique name for the anti-virus scanner setting instance. This field is mandatory.

7 In **Basic Options** tab under **Specify which files to scan**, select one of these options:

Table 5-12 Option definitions — Basic Options

Option	Definition
Scan all files	Scan all files regardless of their type.
Default file types	Scan only the default file types.
Default file types	Scan only the defined file types. Type a three letter file extension. Longer file extensions are included through pattern matching so that "cla" will match ".class" files. Click **Add**. All lower case extensions are converted to upper case extensions. You can enter as many file types as required.

8 Select more scanner options available in **Scanner options**. You can select:

Table 5-13 Option definitions — Scanner options

Option	Definition
Scan archive files (ZIP, ARJ, RAR...)	Scan inside archive files such as .ZIP files.
Find unknown file viruses	To use heuristic techniques to search for unknown viruses.
Find unknown macro viruses	To find unknown viruses in macros.
Enable McAfee Global Threat Intelligence file reputation	This enables the threat intelligence gathered by McAfee Labs that would prevent damage and data theft before a signature update is available. Select the Sensitivity level. The options available are • **very low** — Equivalent to next days DATs. Get tomorrow's protection today. Recommended initial configuration. • **low**— Protection in addition to DATs. • **medium**— Used when the risk of regular exposure to malware is greater than the risk of a false positive. • **high**— Recommended for use in SharePoint repositories which are regularly infected. • **very high**— Recommended for use in on-demand scans on SharePoint repositories. This option should be turned off if the system is not directly connected to the internet, else it impacts the performance significantly.
Scan all files for macros	To scan all files for macros.
Find all macros and treat as infected	To find macros in files and treat them as infected items.
Remove all macros from document files	To remove all macros from the document files.

9 On the **Advanced** tab under **Custom malware categories**, specify the items to be treated as malware. There are two ways to select malware types:

- Select the malware types from the list of checkboxes.
- Select **Specific detection names**, type a malware category, then click **Add**.

  When typing a malware category name, you can use wildcards for pattern matching.

10 Select the **Do not perform custom malware check if the object has already been cleaned** option, if the cleaned items must not be subjected to the custom malware check.

11 In **Clean options**, specify what happens to files that are reduced to zero bytes after being cleaned. Select any one of these options:

- **Keep zero byte file** — To keep files that have been cleaned and is of zero bytes.
- **Remove zero byte file** — To remove any file that has zero bytes after being cleaned.
- **Treat as a failure to clean** — To treat zero-byte files as if they cannot be cleaned, and apply the failure to clean action.

12 In **Packers** tab, select:

- **Enable detection** — To enable or disable the detection of packers.
- **Exclude specified names** — To specify which packers can be excluded from being scanned.
- **Include only specified names** — To specify which packers you want the software to detect.
- **Add** — To add packer names to a list. You can use wildcards to match names.
- **Delete** — To remove packer names you have added. This link is activated if you click **Add**.

13 In **PUPs** tab, select:

- **Enable detection** — To enable or disable the detection of potentially unwanted programs. Click the disclaimer link and read the disclaimer before configuring potentially unwanted programs detection.
- **Select the program types to detect** — To specify whether each type of potentially unwanted programs in the list to be detected or ignored.
- **Exclude specified names** — To specify which potentially unwanted programs can be excluded from being scanned. For example, if you have enabled spyware detection, you can create a list of spyware programs that you want the software to ignore.
- **Include only specified names** — To specify which potentially unwanted programs you want the software to detect. For example, if you enable spyware detection and specify that only named spyware programs should be detected, all other spyware programs are ignored.
- **Add** — To add potentially unwanted programs names to a list. You can use wildcards to match names.
- **Delete** — To delete potentially unwanted programs names that you have added. This link is activated if you click **Add**.

The McAfee Threat Intelligence website contains a list of recent malware names. Use **Search the Threat Library** to view information about specific malware.

14 Click **Save** to return to the policy page.

15 In **Actions to take**, click **Edit**. In these following tabs, specify the anti-virus scanner actions that must be taken if a virus (or virus-like behavior) is detected.

16 Click **Save** to apply the settings and return to the policy settings page.

17 Click **Apply** to configure these settings to a policy.

Configure file filtering settings

Configure settings in a policy to detect files based on their name, type, or size and take necessary actions.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the **File Filtering** scanner.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **File Filtering**.

4 In **Activation**, select **Enable** to activate the file filtering scanner settings for the selected submenu item.

If you are configuring settings for a sub-policy, select **Use configuration from parent policy** to inherit settings from the parent policy.

5 In **Alert Selection**, click:

- **Create** — To create a new alert message when the document on SharePoint server is replaced due to a rule being triggered. See the *Create a new alert* section for more instructions.
- **View/Hide** — To display or hide the preview of the alert message. If the preview is hidden, clicking this link displays it. If the preview is displayed, clicking this link hides it.

You can create alerts only for on-demand policies.

6 In **File filtering rules and associated actions**, from the **Available rules** drop-down menu, select an available rule. If you want to create new file filtering rules, select **<Create new rule...>**. See the *Configure file filtering rules* section for more instructions on how to create new file filtering rules.

7 Click **Change** to specify actions that must be taken when an item triggers the scanner.

8 Click **Delete**, to remove an existing rule from the policy.

9 Click **Apply** to configure these settings to a policy.

Configure DLP and Compliance scanner settings

Configure **DLP and Compliance Scanner** settings in a policy to identify noncompliant data in documents or other items and take necessary actions.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the **DLP and Compliance** scanner.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **DLP and Compliance Scanner**.

4 In **Activation**, select **Enable** to activate the DLP and compliance scanner settings for the selected submenu item.

- By default, all scanner setting options are disabled for **DLP and Compliance Scanner** for sub policies.
- If you are configuring settings for a sub-policy, select **Use configuration from parent policy** to inherit settings from the parent policy.

5 In **Options**, you can use:

- **Include document and database formats** — To scan documents and database formats, for noncompliant content.
- **Scan the text of all attachments** — To scan the text of all attachments.
- **Create** — To create a new alert message when the content of an item is replaced due to a rule being triggered. See the *Create a new alert* section for more instructions.
- **View/Hide** — To display or hide the preview of the alert message. If the preview is hidden, clicking this link displays it. If the preview is displayed, clicking this link hides it.

6 In **DLP and Compliance rules and associated actions**, click **Add rule**.

The **DLP and Compliance Rules** page appears.

7 In **Specify actions for rule**, select a rule group from the **Select rule group** drop-down menu that triggers an action, if one or more of its rules are broken. Each phrase can have a **Score** set for a category, under **DLP and Compliance Scanner Phrase**.

For some rule groups, you might need to specify these options:

- **Threshold score** — To specify the maximum threshold score upon which the scanner triggers.
- **Max Term Count** — To specify the maximum number of times this rule group can be triggered. Exceeding this count triggers the scanner to take the specified action.

The equation for current **Threshold score** = **Score** x Term Count (instance). A rule is triggered when the value equals or exceeds the **Threshold score**.

To understand how **Threshold score** and **Max Term Count** helps in triggering a rule, let us consider an example on Pascal Language dictionary. Consider that you have set the **Score** for the **DLP and Compliance Scanner Phrase** "PAnsiChar" to `5`.

Under **Select rule group**, if you have selected **Pascal Language** dictionary, and set the value for:

- **Threshold score** = 15
- **Max Term Count** = 4

If "PAnsiChar" is found twice in the code, the current threshold score becomes 10. Hence the rule will NOT be triggered.

If "PAnsiChar" is found five times in the code, the current threshold score will still be calculated as **Score** x **Max Term Count** which is 5 * 4 = 20. This value is greater than the defined threshold score. Hence the rule will be triggered.

Consider that you have modified the **Score** for "PAnsiChar" to `8`. If the phrase "PAnsiChar" is found thrice in the code, the current threshold score becomes 24. Now the rule will be triggered as it exceeded the specified **Threshold score**.

If there are multiple rules, the **Threshold score** is the combined value of all the rules for a dictionary.

A rule will be triggered only when the value equals or exceeds the **Threshold score** and is not triggered even if the instance of phrase exceeds the **Max Term Count** value in a document.

8 From **If detected, take the following action:**, select the DLP and compliance scanner actions that must be taken if some content in an item is detected as noncompliant.

9 Click **Save** to apply the settings and return to the policy settings page.

10 Click **Apply** to configure these settings to a policy.

Manage filter settings for a policy

Enable or disable filter options, then specify an appropriate action to take on the detected item when a policy is triggered.

The available filters are:

- **Corrupt Content**
- **Protected Content**
- **Encrypted Content**
- **Signed Content**
- **Password-Protected Files**
- **Scanner Control**

Tasks

- *Configure corrupt content settings* on page 60
  Configure settings in a policy to identify items with corrupt content and take necessary actions.
- *Configure protected content settings* on page 61
  Configure settings in a policy to identify items with protected content and take necessary actions.
- *Configure encrypted content settings* on page 61
  Configure settings in a policy to identify items with encrypted content and take necessary actions.
- *Configure signed content settings* on page 62
  Configure settings in a policy to identify items with signed content and take necessary actions.
- *Configure password-protected files settings* on page 62
  Configure settings in a policy to identify items with are password-protected and take necessary actions.
- *Configure scanner control settings* on page 63
  Configure settings in a policy that defines the nesting level, expanded file size, and maximum scan time that is allowed, when items are scanned.

Configure corrupt content settings

Configure settings in a policy to identify items with corrupt content and take necessary actions.

The content of some documents can become corrupt and cannot be scanned. Corrupt content policies specify how these items with corrupt content are handled when detected.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **Corrupt Content**.

4 For a sub policy, click **Use configuration from parent policy** to inherit all settings from the parent policy.

5 In **Actions**, click **Edit** to specify the filter actions that must be taken when corrupt content is detected.

Click on **Reset** to restore the values in **Corrupt content Actions** to default values.

6 Click **Save** to return to the policy page.

7 Click **Apply** to configure these settings to a policy.

Configure protected content settings

Configure settings in a policy to identify items with protected content and take necessary actions.

Protected content policies specify how items with protected content are handled when detected.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **Protected Content**.

4 For a sub policy, click **Use configuration from parent policy** to inherit all settings from the parent policy.

5 In **Actions**, click **Edit** to specify the filter actions that must be taken when protected content is detected.

Click on **Reset** to restore the values in **Protected content Actions** to default values.

6 Click **Save** to return to the policy page.

7 Click **Apply** to configure these settings to a policy.

Configure encrypted content settings

Configure settings in a policy to identify items with encrypted content and take necessary actions.

Some documents can be encrypted to prevent access by unauthorized parties. Encrypted content uses a key and encryption mathematical algorithms to decrypt it. Encrypted content policies specify how items with encrypted content are handled when detected.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **Encrypted Content**.

4 For a sub policy, click **Use configuration from parent policy** to inherit all settings from the parent policy.

The encrypted content settings are enabled by default.

5 In **Actions**, click **Edit** to specify the filter actions that must be taken when encrypted content is detected.

Click on **Reset** to restore the values in **Encrypted content Actions** to default values.

6 Click **Save** to return to the policy page.

7 Click **Apply** to configure these settings to a policy.

Configure signed content settings

Configure settings in a policy to identify items with signed content and take necessary actions.

Signed content policies specify how items with signed content are handled when detected.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **Signed Content**.

4 For a sub policy, click **Use configuration from parent policy** to inherit all settings from the parent policy.

5 In **Actions**, click **Edit** to specify the filter actions that must be taken when signed content is detected.

Click on **Reset** to restore the values in **Signed content Actions** to default values.

6 Click **Save** to return to the policy page.

7 Click **Apply** to configure these settings to a policy.

Configure password-protected files settings

Configure settings in a policy to identify items with are password-protected and take necessary actions.

Password-protected files cannot be accessed without a password and cannot be scanned. Password-protected policies specify how these items are handled when detected.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **Password-Protected Content**.

4 For a sub policy, click **Use configuration from parent policy** to inherit all settings from the parent policy.

5 In **Actions**, click **Edit** to specify the filter actions that are taken.

Click on **Reset** to restore the values in **Password-Protected content Actions** to default values.

6 Click **Save** to return to the policy page.

7 Click **Apply** to configure these settings to a policy.

Configure scanner control settings

Configure settings in a policy that defines the nesting level, expanded file size, and maximum scan time that is allowed, when items are scanned.

Task

For option definitions, click **?** in the interface.

1 From **Policy Manager**, select a submenu item that has the scanner.

The policy page for the submenu item appears.

2 Click **Master policy** or any sub-policy you want to configure, then click **List All Scanners** tab.

3 Click **Scanner Control**.

4 For a sub policy, click **Use configuration from parent policy** to inherit all settings from the parent policy.

5 In **Options**, click **<create new set of options>**.

6 In **Instance name**, type a unique name for the scanner control filter setting instance. This field is mandatory.

7 In **Maximum nesting level**, specify the level to which the scanner should scan, when an attachment contains compressed files, and other compressed files within. You can specify a value from 2–100, where the default value is 100.

8 In **Maximum expanded file size (MB)**, specify the maximum size allowed for a file when it is expanded for scanning. You can specify a value from 1–2047, where the default value is 500.

Maximum scan time (minutes) is the maximum time allowed to scan any file. This value is taken from SharePoint Anti-Virus settings.

9 Click **Save** to return to the policy page.

10 In **Alert selection**, you can select which alert to use when a scanner control option is triggered. You can use:

- **Create** — To create a new alert message for this policy.
- **View/Hide** — To display or hide the alert text. If the text is hidden, clicking this link displays it. If the text is displayed, clicking this link hides it.

11 In **Actions**, click **Edit** to specify the actions to take, if the value exceeds the specified settings for maximum nesting level, maximum expanded file size and maximum scanning time.

12 Click **Save** to return to the policy page.

13 Click **Apply** to configure these settings to a policy.

6 Settings and diagnostics

Configure the feature enablement and disablement, feature configuration, feature administration and logs for the software based on your organization's security policy.

To modify or view the product settings, from the product's user interface, click **Settings & Diagnostics**. This table briefly explains when to configure these settings:

Table 6-1 Settings & diagnostics

Use...	To...
Detected Items	Configure and manage local quarantine database activities such as purge and optimization. It also has options to specify item size, query size and item age.
User Interface Preferences	Define settings in the **Dashboard** such as the refresh rate, report settings, unit scale of graphics, reporting interval, graph and chart settings.
Diagnostics	Define settings for debug, error reporting, event and product logs, including information on how big the logs are and where they are stored. Diagnostics settings include: • **Debug Logging** • **Error Reporting Service** • **Event Logging** • **Product Log**
Product Log	View the **Product Log** and filter the output by date, type or description.
Import and Export Configuration	Set up your current product server with the same configurations as one already built, restore default settings, or create SiteLists to point to DAT download locations.
DAT Settings	Specify the maximum number of detection definition files to maintain instead of all DAT's.
User Settings	Define what to do with an item when the scanner fails to scan an item in on-access scan. The options are: • **Allow Through** • **Prevent Upload** It also has options to specify sharepoint scanner interval, scanner count, quarantine size and also add application pools.

If you modify any of these settings, make sure you click **Apply** to save the changes. The background color behind **Apply**, changes to:

- Yellow — If you have changed the existing setting or the change is still not applied.
- Green — If you have not changed the existing setting or the change is applied.

Contents

- *Configure local quarantine database for detected items*
- *User interface preference settings*
- *Diagnostics settings*
- *View product logs*
- *Import and export configuration settings*
- *Configure DAT settings*
- *Configure user settings*

Configure local quarantine database for detected items

Specify repository settings to store the quarantined items detected by the software.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Detected Items**.

The **Detected Items** page appears.

2 From the **Local Database** section, you can use:

Table 6-2 Option definitions

Option	Definition
Specify location of database	To change the database location for storing the quarantined items detected by the software. The default database location is the **<Install Folder>**.
Database location	To specify the database location path where items detected by the software can be stored. You can select: • **<Install Folder>** — To create the database sub-folders under the product installation directory. • **<System Drive>** — To create the database sub-folders in operating system install drive `C:\` directory. • **<Program Files>** — To create the database sub-folders under the Windows `C:\Program Files (x86)` directory. • **<Windows Folder>** — To create the database sub-folders under the `C:\Windows` directory. • **<Full Path>** — To specify the complete path of the local database. Specify the sub-folder path in the field next to the drop-down list.
Maximum item size (MB)	To specify the maximum size of a quarantined item that can be stored in the database. You can specify a value from 1 to 100, where the default value is 100. If the maximum item size is more than 100 then it will not be quarantined.
Maximum query size (records)	To specify the maximum number of records or quarantined items you can query from the **Detected Items** page. You can specify a value from 1 to 20000, where the default value is 1000.

Table 6-2 Option definitions *(continued)*

Option	Definition
Maximum item age (days)	To specify the maximum number of days an item will be stored in the local quarantine database, before being marked for deletion. You can specify a value from 1 to 365, where the default value is 14.
Purge of old items frequency	To specify how frequently old items that are marked for deletion are deleted from the product database. The default value is set to **Daily**. For more information on removing old items marked for deletion see *Purge and optimize*.
Optimization frequency	To recover the disk space taken up by deleted database records. Based on the value set under **Maximum item age (days)**, old records will be deleted if you have scheduled a purge task. To optimize and shrink the database, schedule an optimization task. The default value is set to **Not scheduled**. • Always schedule an optimization task a few hours after you perform the purge task. • For more information on removing old items marked for deletion see *Purge and optimize*.
Edit Schedule	To modify the schedule of the purge or optimization task. Click **Save** after modifying the schedule.

3 Click **Apply** to save the settings.

You have now successfully configured your product server to start quarantining detected items on to the local database.

User interface preference settings

Define settings in the **Dashboard** such as the refresh rate, report settings, unit scale of graphics, reporting interval, graph and chart settings.

Configure dashboard settings

Configure settings in the **Dashboard** such as the statistics, unit scale of graph, items to view in the **Recently Scanned Items**, and status reporting interval.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **User Interface Preferences**.

The **User Interface Preferences** page appears.

2 Click **Dashboard Settings** tab. You can use:

Table 6-3 Option definitions

Option	Definition
Automatic refresh	To specify whether the information shown on the **Dashboard** | **Statistics** counter should be refreshed automatically. Always enable this to see the updated statistics on dashboard.
Refresh rate (seconds)	To specify the duration (in seconds) at which the information on the dashboard should be refreshed. You can specify a value from 30 to 3600, where the default value is 60.
Maximum recently scanned items	To specify the maximum number of items to appear in the **Dashboard** | **Reports** | **Recently Scanned Items** section. You can specify a value from 10 to 100, where the default value is 20.
Graph scale (units)	To specify the measurement units for the scale of the bar graph that is generated on the **Dashboard** | **Graph** section. You can specify a value from 100 to 500, where the default value is 100.
Number of hours to report for	To specify the report generation interval in hours. You can specify a value from 1 to 24, where the default value is 7.

3 Click **Apply** to save the settings.

Configure graph and chart settings

Configure settings in the **Dashboard** | **Graph** section to enhance the graph and chart settings.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **User Interface Preferences**.

2 Click **Graph and Chart Settings** tab. You can use:

Table 6-4 Option definitions

Option	Definition
3D	To specify whether you want the dashboard graph to be displayed as a three-dimensional (3D) graph.
Draw transparent	To specify whether the bars in a three-dimensional bar graph should appear solid or transparent. A solid bar hides part of any bar behind it. A transparent bar allows you to look through it and see other transparent bars behind it.
Anti-alias	To specify whether you want to use anti-aliasing techniques when displaying pie charts. When anti-aliasing is used, pie charts have smoother curves. If anti-aliasing is not used, pie chart curves appear jagged.
Explode pie	To specify whether the segments should remain within the circle of the pie chart or be shown with exploded segments.
Pie angle (degrees)	To specify the angle to use when displaying pie charts. You can specify a value from 1 to 360, where the default value is 45.

3 Click **Apply** to save the settings.

Diagnostics settings

Determine the causes of symptoms and the errors encountered while using McAfee Security for Microsoft SharePoint.

In the **Settings & Diagnostics** | **Diagnostics** page, you can use:

- **Debug Logging** — To configure debug logging settings such as specifying the debug log level, maximum file size limit of the log file, and the file location.
- **Error Reporting Service** — To configure settings to determine whether to catch exceptions such as crashes.
- **Event Logging** — To configure settings to capture product or event related logs based on information, warnings or errors.
- **Product Log** — To configure settings for the product log file (`productlog.bin`). Changes made to this setting will be reflected on the **Settings & Diagnostics** | **Product Log** page.

Configure debug log settings

Configure settings to specify the debug log level, maximum file size limit of the log file, and the log file location. Use these settings when you want to troubleshoot an issue with the product and provide the logs to McAfee Technical Support for further analysis.

Configure **Debug Log** settings for troubleshooting purposes and only for a limited duration. Once you capture sufficient logs for troubleshooting, set the value for **Level** to **None**. Using debug logging indiscriminately could fill up the hard disk space and affect the overall performance of the server. Enable it for a limited duration as advised by an authorized personnel (McAfee Technical Support Engineer).

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Diagnostics**.

The **Diagnostics** page appears.

2 In the **Debug Logging** tab, you can use:

Table 6-5 Option definitions

Option	Definition
Level	To enable or disable debug logging and specify the level of information that should be captured in the debug log file. You can select: • **None** — To disable debug logging. • **Low** — To log critical events such as errors, exceptions, and return values of functions in the debug log file. Select this if you want to keep a low size for the debug log file. • **Medium** — To log events mentioned in the **Low** state and additional information that could be of help to the technical support team. • **High** — To log all critical errors, warnings and debug messages in the debug log file. It contains information about all activities performed by the product. This is the most detailed level of logging supported by the product.
Enable size limit	If you want to specify a maximum file size limit for each debug log file.

Table 6-5 Option definitions *(continued)*

Option	Definition
Specify maximum file size	To specify how large the debug log files can be. You can specify a value from 1 KB to 2000 MB. If the debug log files exceed the specified file size, older events will be rewritten due to circular logging, where new log entries are added to the file by deleting the oldest log entries.
Enable debug logging	If you want to modify the default debug file logging location.
Specify file location	To specify the debug log file location path where events triggered by the product can be stored. You can select: • **<Desktop>** — To create the debug log files on the desktop. • **<Install Folder>** — To create the debug log files under the product installation directory. • **<System Drive>** — To create the database sub-folders in operating system install drive `C:\` directory. • **<Program Files>** — To create the database sub-folders under the Windows `C:\Program Files (x86)` directory. • **<Windows Folder>** — To create the debug log files under the `C:\Windows` directory. • **<Full Path>** — To store the debug log files in the complete path specified in the adjacent text box. To store the debug log files to a custom location or sub-folder, specify the sub-folder name or path in the field next to the drop-down list.

Make sure that the folder that collects the debug logs is provided "Write" permissions for the NETWORK SERVICE account.

3 Click **Apply** to save the settings.

You have now successfully configured the debug log settings, that you can use for troubleshooting.

Configure error reporting settings

Configure settings to report product related errors or exceptions to McAfee.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Diagnostics**.

The **Diagnostics** page appears.

2 Click the **Error Reporting Service** tab. You can use:

Table 6-6 Option definitions

Option	Definition
Enable	To enable or disable the error reporting service.
Catch exceptions	To capture information about events causing exceptions.
Report exceptions to user	To specify whether exceptions should be reported to the administrator.

3 Click **Apply** to save the settings.

Configure event log settings

Configure settings to log the product events in the **Product Log** and Windows Event Viewer.

An event is a possible action that you perform, which is monitored by the software. **Event Logging** provides information useful for diagnostics and auditing. The different classes of events are:

- Error
- Information
- Warning

This allows you to more easily obtain information on problems that occur.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Diagnostics**.

The **Diagnostics** page appears.

2 Click **Event Logging** tab. You can use:

Table 6-7 Option definitions

Option	Definition
Product Log	To log the product events in the **Product Log**. These events can be viewed from **Settings & Diagnostics** | **Product Log** | **View Results** section.
Event Log	To log the product events under Windows Event Viewer. To find the product related events in the Windows Event Viewer: 1 Go to **Event Viewer (Local)** | **Windows Logs** | **Application**. 2 In the **Application** pane, product related events appear as **McAfee PortalShield** under the **Source** column.
Write information events	To log events that are categorized as **Information**.
Write warning events	To log events that are categorized as **Warning**.
Write error events	To log events that are categorized as **Error**.

3 Click **Apply** to save the settings.

Configure product log settings

Configure the product settings by specifying the required parameters to generate product logs.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Diagnostics**.

The **Diagnostics** page appears.

2 Click the **Product Log** tab. You can use:

Table 6-8 Option definitions

Option	Definition
Location	If you want to configure a location to store the product log. Select **Enable** to specify a custom location.
Specify database location	To specify the product log file location path where product log events can be stored. You can select: • **<Desktop>** — To create the debug log files on the desktop. • **<Install Folder>** — To create the debug log files under the product installation directory. • **<System Drive>** — To create the database sub-folders in operating system install drive `C:\` directory. • **<Program Files>** — To create the database sub-folders under the Windows `C:\Program Files (x86)` directory. • **<Windows Folder>** — To create the debug log files under the `C:\Windows` directory. • **<Full Path>** — To store the debug log files in the complete path specified in the adjacent text box. To store the product log file to a custom location or sub-folder, specify the sub-folder name or path in the field next to the drop-down list.
Filename	If you want to specify a different file name to store the product log. Select **Enable** to specify a custom file name.
Specify database filename	To specify a custom file name for the product log. The default file name is `productlog.bin` under `<Install Folder>` directory. If you modify the default product log file name or path, the log entries in the **Settings & Diagnostics** | **Product Log** page will be reset and older log entries will not appear.
Size Limit	If you want to specify a different size limit for the product log file. Select **Enable database size limit** to specify a custom file size.
Specify maximum database size	To specify how large the product log file can be. You can specify a value from 1 KB to 2000 MB. If the product log file exceeds the specified file size, older log events will be rewritten due to circular logging, where new log entries are added to the file by deleting the oldest log entries.
Limit age of entries	If you want the product log entries to be deleted after a set period of time.
Specify maximum age of entry (days)	To specify how many days an entry should remain in the product log file before it is deleted. You can specify a value from 1 to 365.
Query Timeout	If you want to limit the amount of time allowed for answering a product log query. Select **Enable** to specify the duration.
Specify query timeout (seconds)	To specify the maximum number of seconds allowed, when responding to a product log query. You can specify a value from 1 to 3600.

3 Click **Apply** to save the settings.

You have now successfully configured settings for the **Product Log** page.

View product logs

View the product's health using log entries about event levels such as information, warnings, and errors. For example, you can view information on when a task initiated or ended, product service errors and so on.

You can use the available search filters to find log entries that are of interest to you.

To modify settings related to the product log query page, go to **Settings & Diagnostics** | **Diagnostics** | **Product Log**.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Product Log**. The **Product Log** page appears.

2 From the **Product Log** section, you can use:

Table 6-9 Option definitions

Option	Definition
ID	To specify the number which identifies a specific product log entry.
Level	To select **Information**, **Warning** or **Error** from the drop-down list, depending on the type of log you want to view.
Description	To specify a relevant description. For example, if you want to view logs based on service start or stop, type: `*service*`
All Dates	To include events from all dates which is based on the entry in the product log file.
Date Range	To search for an event within a defined date range according to your requirements. Here you can specify the date, month, year and time against the parameters **From** and **To**. You can also use the calendar icon to specify a date range.
Clear Filter	To return to the default search settings.
Export to CSV File	To export and save information about all events returned by the search in a `.CSV` format. If there are thousands of events in the log, instead of navigating through multiple pages, you can use this option to download these events to a file in CSV format and later generate custom reports in Microsoft Excel. • If you do not find a specific field in the search result of the CSV file, make sure to enable the required field in the **Columns to Display** option. • Use the Import Data option in Microsoft Excel, to open the CSV file in a different locale.

Table 6-9 Option definitions *(continued)*

Option	Definition
Columns to display	To select or deselect column headers to be listed in the **View Results** pane.
Views **Per Page**	To specify the maximum number of logs you want to view per page. The options are: • **10** • **20** • **50** • **100**

3 Click **Search**.

The maximum number of records that can be stored in the product log is based on the log file size.

A list of events matching your search criteria are displayed in the **View Results** section.

Import and export configuration settings

Configure settings to export existing product configuration (settings and policies) for import and use on another McAfee Security for Microsoft SharePoint server. Also import sitelists to specify the location from where automatic updates are downloaded.

From the product's user interface, click **Settings & Diagnostics** | **Import and Export Configuration**. In the **Import and Export Configurations** page, you can use these tabs:

- **Configuration** — To export, import or restore product settings.

Table 6-10 Configuration tab — Option definitions

Option	Definition
Export	To copy the software configuration (settings and policies) of this server and save it to a location from where it can be imported by other McAfee Security for Microsoft SharePoint servers. The default software configuration file is `McAfeeConfigXML.cfg`.
Restore Default	To reset the settings for your product to maximum performance. If you have customized the product, restore default will reset all the settings to the default settings.
Browse	To locate the configuration file (`McAfeeConfigXML.cfg`) that you want to import.
Import	To apply the settings of another McAfee Security for Microsoft SharePoint server to this server. • You must import settings across the same product version. For example, you must not import settings from McAfee Security for Microsoft SharePoint 2.5 server to a 3.0 product server. • If you import configurations from a different farm, then you have to re configure the on demand scan tasks.

- **SiteList** — To import sitelists that specify the location from where automatic updates are downloaded.

Table 6-11 SiteList tab — Option definitions

Option	Definition
Browse	To locate the sitelist file (`SiteList.xml`) that you want to use.
Import	To apply the sitelist configuration settings specified in the file, to download DAT updates.

Import product configuration from another server

Apply the product configuration settings from another server to this server.

You must import settings across the same product version. For example, you must not import settings from McAfee Security for Microsoft SharePoint 2.5 server to a 3.0 product server.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Import and Export Configuration**.

The **Import and Export Configurations** page appears.

2 Click the **Configuration** tab.

3 From the **Import Configuration** section, click **Browse** to locate the configuration file. The default name of the configuration file is `McAfeeConfigXML.cfg`.

4 Click **Import**.

A dialog box appears with the message **The operation completed successfully**.

5 Click **OK**.

You have now successfully imported configuration settings from another product server to this server.

Export your product configuration

Export the configuration of a the product server and save it to a location, where it can be imported by other McAfee Security for Microsoft SharePoint servers.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **Import and Export Configuration**.

The **Import and Export Configurations** page appears.

2 Click the **Configuration** tab.

3 Click **Export**.

4 Specify a location where to save the configuration file. The default name of the configuration file is `McAfeeConfigXML.cfg`.

5 Click **Save**.

You have now successfully exported your existing product settings and policies to a configuration file, that can be imported by other McAfee Security for Microsoft SharePoint servers.

Import a sitelist

Import a sitelist that specifies the location, from where automatic updates are downloaded.

A sitelist specifies from where automatic updates are downloaded. By default, the software uses **SiteList Editor** that points to a McAfee URL for automatic updates.

If your product server is managed by McAfee ePO, the sitelist from ePO is used to perform automatic updates. If you are not using ePO to manage your product server, create a sitelist that points your McAfee Security for Microsoft SharePoint server to a local repository.

Task

For option definitions, click **?** in the interface.

1 Click **Settings & Diagnostics** | **Import and Export Configuration**. The **Import and Export Configurations** page appears.

2 Click the **SiteList** tab.

3 From the **Import SiteList** section, click **Browse** to locate the sitelist file `SiteList.xml`. This file contains information about the repository settings such as repository name, server URL, and so on.

You can find the `SiteList.xml` file under `C:\ProgramData\McAfee\Common FrameWork\` directory. The **SiteList Editor** application under **Start** | **All Programs** | **McAfee** | **McAfee Security for Microsoft SharePoint** uses this file to display the repository settings in the application.

4 Click **Import**.

A dialog box appears with the message **The operation completed successfully**.

5 Click **OK**.

You have now successfully imported the sitelist that points to a new repository location, to download product updates.

Configure DAT settings

Specify the number of old DATs that can be retained in your system.

DAT files are the detection definition files, also referred to as signature files, that identify the code anti-virus and/or anti-spyware software detects to repair viruses, trojan horses and Potentially Unwanted Programs (PUPs). For glossary information on .DAT files, go to: http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx#dat.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **DAT Settings**.

The **DAT Settings** page appears.

2 Use **Maximum number of old DATs** to specify the maximum number of DAT generations that shall be preserved in the system during regular updates, excluding the DAT that comes with the product release.

The software retains the latest DATs with old DATs under `<Install Folder>\bin\DATs` directory.

3 Whenever a new DAT update occurs, the software verifies the number of available DATs. If the available DATs count exceeds the DAT retention value, the oldest DAT will be deleted. You can specify a value from 3 to 10, where the default value is 10.

4 Click **Apply** to save the settings.

Configure user settings

Configure settings for on-access scan here. When ever user uploads or downloads files, on-access scanning is triggered and the software checks for detections.

Task

For option definitions, click **?** in the interface.

1 From the product's user interface, click **Settings & Diagnostics** | **User Settings**.

The **User Settings** page appears.

2 From **On-Access Settings**, you can choose:

Table 6-12 Option definitions

Option	Definition
On Scan Failure	Specify if you want to allow the items through or prevent upload, if scanning fails. • **Allow Through** • **Prevent Upload** By default, **On Scan Failure** is set to **Prevent Upload**. We recommend that you do not change this setting.
Retrieve SharePoint AV Settings Every (minutes)	Specify the time (in minutes) to retrieve the anti-virus settings from the SharePoint server. We recommend that you specify a lesser duration so that the dashboard synchronizes with your SharePoint anti-virus settings.
Maximum Quarantine Size	Specify the maximum size of the quarantined item in MB or KB. You can specify a value from `1` to `102400` KB or `1` to `100` MB, where the default value is `3125` KB.
Maximum Scanner Count	Specify the maximum number of scanner counts. You can specify a value from `1` to `5`. The default value is `5`. Scanner count specifies the number of threads at a time that the software will take up for processing.
Add ApplicationPool(s) to be Recycled	Specify an application pool which you want to add to the product. Application pools are used to separate processes that share same configuration or application boundaries. They are used to isolate web applications for better security, reliability and performance. When McAfee Security for Microsoft SharePoint is installed, it creates an application pool *MSMSAppPool* so that it does not affect the SharePoint server. If you have any custom application pools for your organization and you want to add them to the product server, you can add by using this option.

Table 6-12 Option definitions *(continued)*

Option	Definition
Add Application pool	Specify an application pool in **Add ApplicationPool(s) to be Recycled** and click **Add**. Add all the application pools where SharePoint sites are running.
Existing ApplicationPool(s) to be Recycled:	Shows the list of application pools configured for this SharePoint server.
Remove Application pool	Select an application pool from the **Existing ApplicationPool(s) to be Recycled:** and click **Remove** to exclude application pools that are no longer required. To select more than one application pool, use Ctrl+click or Shift+click.

3 Click **Apply** to save the settings.

You have now successfully configured the on-access settings for your product.

7 Program Maintenance

Perform the maintenance tasks such as repair, purge, or remove McAfee Security for Microsoft SharePoint.

Contents

- *Repair the installation*
- *Purge and optimize*
- *Restore default configuration*
- *Uninstall the software*

Repair the installation

You can resolve the installation errors in the program by fixing corrupt or missing files, shortcuts and registry entries.

You can also repair the installation from the folder containing the install files, by clicking `setup.exe`. Repairing an installation will revert to the default configuration settings.

Task

1 Click **Start** | **Settings** | **Control Panel**.

2 Double-click **Add/Remove Programs**. The **Add/Remove Program** window appears.

3 Select **McAfee Security for Microsoft SharePoint** from the list and click **Change**. The installation wizard appears followed by the **Application Maintenance** dialog box with the **Repair** option selected by default.

4 Click **Next**. The **Database Account** dialog box appears.

5 Modify the **Account Information** as required.

If the user credentials cannot be resolved by the server, a warning dialog box appears prompting you to check your credentials.

6 Verify if you have entered correct credentials. Click **OK**, then click **Next** to override the warning and proceed with the repair process with unresolved account information.

A repair installation will reset the DAT and engine files to the version originally installed by the product. It is recommended to run an update after installation.

The **Ready to repair the Application** dialog box appears.

7 Click **Next**. The **Updating System** window appears. After McAfee Security for Microsoft SharePoint is updated, a confirmation message is displayed.

8 Select or deselect the following options as required and click **Finish**.

- **Launch User Interface** — To launch the graphical user interface of the product.
- **Update Now** — To download the latest product updates and to ensure you are running the most current security to combat the ever-evolving threats.

Purge and optimize

Remove old items marked for deletion from the database and use optimization task to recover disk space being taken up by deleted database records.

Task

1 From the product's user interface, click **Settings & Diagnostics** | **Detected Items**.

The **Detected Items** page appears.

2 From the **Local Database** section, you can use:

- **Purge of old items frequency** — To specify how frequently old items that are marked for deletion are deleted from the database. The default value is set to **Daily**.
- **Optimization frequency** — To recover the disk space taken up by deleted database records. Based on the value set under **Maximum item age (days)**, old records will be deleted if you have scheduled a purge task. To optimize the database, schedule an optimization task.

Always schedule an optimization task a few hours after you perform the purge task.

3 Click **Edit Schedule** to modify the schedule. You can choose a time based on the options.

- **Not scheduled** — Select this if you have not decided on when to perform the purge or optimization.
- **Once** — Specify the date and time to schedule the purge or optimization once.
- **Hours** — Select this to schedule the purge or optimization based on hours.
- **Days** — Select this to schedule the purge or optimization based on how often it must occur in a week.
- **Weeks** — Select this to schedule the purge or optimization based on how often it must occur in a month.
- **Months** — Select this to schedule purge or optimization based on how often it must occur in a year.

These tasks should be performed on a regular basis to maintain adequate free space in the database.

Restore default configuration

Restore the product to its default configuration.

Task

1 From the product's user interface, click **Settings & Diagnostics** | **Import and Export Configuration**. The **Import and Export Configurations** page appears.

2 From the **Configuration** tab, click **Restore Default**.

Restoring the default settings removes all policy settings and sub-policies configured. It is recommended that you take a backup of existing settings, to restore the settings later.

A dialog box appears asking you to confirm the settings.

3 Click **OK**.

A dialog box appears confirming that the default configuration settings are applied.

You have now successfully restored your McAfee Security for Microsoft SharePoint server to default configuration settings for maximum performance.

Uninstall the software

Remove or uninstall the software from the server.

You can also remove the software from the folder containing the install files by double-clicking `setup.exe`.

Task

1 Click **Start** | **Settings** | **Control Panel**.

2 Double-click **Add/Remove Programs**. The **Add/Remove Program** window appears.

3 Click **McAfee Security for Microsoft SharePoint** from the list, then click **Uninstall**.

Alternatively, you can double-click **McAfee Security for Microsoft SharePoint** from the list.

4 Click **Yes**. A progress bar appears displaying the status.

After uninstalling, the product name is removed from the **Add/Remove Programs** list.

8 Integrating with ePolicy Orchestrator

You can integrate and manage the product using ePolicy Orchestrator management software.

McAfee ePO provides a scalable platform for centralized policy management and enforcement on your McAfee security products and systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

You can integrate this product with McAfee ePO 4.5, 4.6, and 5.0.

For instructions about setting up and using McAfee ePO, see the product guide for your version.

Contents

- *Prerequisites*
- *Check in the software package*
- *Install the software extensions*
- *Migrate the policies from older version*
- *Deploy the software to clients*
- *Manage Policies*
- *Create and schedule tasks*
- *Queries and reports*
- *Filter events*
- *Remove the software*

Prerequisites

Set up your environment before you integrate the product with ePolicy Orchestrator

- Use administrator credentials of the ePolicy Orchestrator server.
- Add manageable nodes to the ePolicy Orchestrator server on which you want to deploy McAfee Security for Microsoft SharePoint. See ePolicy Orchestrator product documentation for instructions.
- Deploy McAfee Agent on your managed nodes running Microsoft SharePoint. See the McAfee Agent product documentation for installation instructions.
- If you're upgrading from a previous release, uninstall any earlier versions of the product other than McAfee Security for Microsoft SharePoint 2.5 patch 1.
- Make sure you have administrator credentials for each SharePoint server in single server mode or farm environment.
- Choose open/unused port on the server where you want to host the McAfee Security for Microsoft SharePoint site.

Check in the software package

Check in the McAfee Security for Microsoft SharePoint deployment package to the ePolicy Orchestrator server.

Task

For option definitions, click **?** in the interface.

1 Log on to ePolicy Orchestrator server as administrator.

2 Click **Menu** | **Software** | **Master Repository**, then click **Action** | **Check In Package**.

3 In the **Package** step, select **Product or Update (.zip)**, click **Browse** and browse to the .zip file containing the software package, then click **Next**.

4 In the **Package Options** step, select **Current** as the branch, then click **Save**.

Install the software extensions

Install the software extensions on the ePolicy Orchestrator server.

Even if you have a previous version of the software extension, this task adds the McAfee Security for Microsoft SharePoint 3.0 extension to the list. You can retain the previous extensions or remove them, as needed.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Software** | **Extensions**, then click **Install Extension**.

3 Click **Browse** and browse to the .zip file containing the policy extension (`MSMS30PolicyEx_0409.zip` for English), then click **OK**.

Install the report extension and the help extension in the same way.

Migrate the policies from older version

When you upgrade the software, migrate existing policies from older versions to McAfee Security for Microsoft SharePoint version 3.0.

Task

For option definitions, click **?** in the interface.

1 Browse to the folder containing the `MSMS_ePOUpgrade.zip`, then extract it.

Make sure that all files in the .zip are extracted to the same folder.

2 On the command prompt, navigate to the folder where the .zip file is extracted, and run the `MSMSePOUpgrade.exe` command.

3 Type the ePolicy Orchestrator database password, then press `Enter`.

4 Type the ePolicy Orchestrator SQL named instance if created during the server installation, otherwise leave it blank. Then press `Enter`.

The policy upgrade process starts. Wait for it to complete.

On successful completion, a confirmation message appears. See `EPODebugTrace.txt` in the current directory for log details. Press `Enter` to exit.

- Verify that the policies are upgraded: In the ePolicy Orchestrator console, navigate to **Policy Catalog**, select the product as **McAfee Security for Microsoft SharePoint 3.0.0**, then look for upgraded policies suffixed with **(Upgraded)**. For example, **My Default (Upgraded)**.
- Assign the custom policies to the required systems, otherwise the McAfee default policies are enforced.

Deploy the software to clients

Deploy the software to Microsoft SharePoint client systems.

Before you begin
Migrate existing policies from older versions to McAfee Security for Microsoft SharePoint 3.0.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select the required group or systems.

When upgrading the software, make sure that you select all required systems.

3 Complete these steps according to your version of ePolicy Orchestrator:

Version 4.5	Version 4.6 and Version 5.0
1 Click the **Client Tasks** tab, then click **New Task**. The **Client Task Builder** screen appears. 2 Type a name for the task, and any notes. 3 Select **Product Deployment** as the task type, then click **Next**. 4 Select **Windows** as a target platform.	1 Click the **Assigned Client Tasks** tab, then click **Actions** | **New Client Task Assignment**. The **Client Task Assignment Builder** screen appears. 2 In **Product**, select **McAfee Agent**. 3 In **Task Type**, select **Product Deployment**. 4 Click **Create New Task**. The **Client Task Catalog** screen appears. 5 Type a name for the task, and any notes. 6 Select **Windows** as a target platform.

4 In **Products and components**, select **McAfee Security for Microsoft SharePoint - xxxxxxxx 3.0.0.xxxx**, select **Install** as action, select the language, then click **Save**.

Type the credentials for the system that has the SharePoint server installed in ePolicy Orchestrator command line.

- `REMOTESQLUSER = "DomainName\UserName or HostName\UserName"`
- `REMOTESQLPWD = "password"`
- `IISPORT = 45900 (Optional)`

5 Schedule the task to run immediately, then click **Next** to view a summary of the task.

6 Review the summary of the task, then click **Save**.

7 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

8 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

On successful execution of this task, the software is deployed to the selected systems.

Manage Policies

McAfee Security for Microsoft SharePoint policies provide options to configure the policies, feature enablement and disablement, feature configuration, feature administration, and logs.

These policy settings are nearly identical to those you can access from the **Policy Manager** and **Settings and Diagnostics** tab in the product's user interface.

You can find policies on the **Policy Catalog** page under the **McAfee Security for Microsoft SharePoint** product.

- **Scanner Settings**— Modify settings for on-access or on-demand policies.
- **Settings and Diagnostics**— Modify settings related to feature enablement and disablement, feature configuration, feature administration, and logs.

Modify the policies with your preferences, then assign them to groups of managed Microsoft SharePoint systems or to a single system. For generic information about policies, see the product guide for your version of the ePolicy Orchestrator software.

Tasks

- *Create or modify policies* on page 86
  Create or modify McAfee Security for Microsoft SharePoint policies from the **Policy Catalog**.
- *Assign policies* on page 87
  When you've created or modified the product policies with the required settings, assign each of them to the required Microsoft SharePoint systems that are managed by ePolicy Orchestrator.

Create or modify policies

Create or modify McAfee Security for Microsoft SharePoint policies from the **Policy Catalog**.

Alternatively, you can create or modify these policies from the **System Tree**, while assigning policies to selected systems. See the product guide for your version of the ePolicy Orchestrator software for more information.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the **Policy Catalog**, select **McAfee Security for Microsoft SharePoint 3.0.0** as the product, then select the required policy as the category.

3 Perform this step as required:

To create a policy	To modify a policy
Click **New Policy**, type a name for the policy, then click **OK**.	Click the policy that you want to modify.

4 Modify the policy settings as required, then click **Save**.

The policy settings are updated and the new policy (when created) appears in the **Policy Catalog**.

Assign policies

When you've created or modified the product policies with the required settings, assign each of them to the required Microsoft SharePoint systems that are managed by ePolicy Orchestrator.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Navigate to the **System Tree**, select a required group or systems, then click the **Assigned Policies** tab.

3 Select **McAfee Security for Microsoft SharePoint 3.0.0** from the products list, locate the required policy, then click **Edit Assignment** next to the policy.

4 (Optional) Select a policy, then click **Edit Policy** to modify the policy settings. Click **New Policy** to create a new policy based on the selected category.

Alternatively, you can also modify or create a policy from the **Policy Catalog**.

5 Select the policy to assign, select appropriate inheritance options, then click **Save**.

The policy enforcement occurs in the next agent-server communication. Click **Wake Up Agents** to enforce policies immediately.

Create and schedule tasks

Create client tasks on your Microsoft SharePoint systems to schedule automated actions.

Tasks

- *Schedule automatic updates* on page 88
  Schedule automatic updates to keep your software up-to-date with the latest anti-virus definitions (DATs) and anti-virus scanning engine.
- *Schedule on-demand scan* on page 89
  Schedule an on-demand scan to scan your Microsoft SharePoint servers to find a threat, vulnerability, or other potentially unwanted code.
- *Schedule an optimization task* on page 89
  Schedule an optimization task to recover disk space taken up by deleted database records.
- *Schedule purge old DATs task* on page 90
  Schedule a purge old DATs task to delete old DAT's.
- *Schedule purge task* on page 91
  Schedule a purge task to delete old items from the database.

Schedule automatic updates

Schedule automatic updates to keep your software up-to-date with the latest anti-virus definitions (DATs) and anti-virus scanning engine.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select the required group or systems.

3 Complete these steps according to your version of ePolicy Orchestrator:

Version 4.5	Version 4.6 and Version 5.0
1 Click the **Client Tasks** tab, then click **New Task**. The **Client Task Builder** screen appears. 2 Type a name for the task, and any notes. 3 Select **AutoUpdate Task (McAfee Security for Microsoft SharePoint 3.0.0)** as the task type, then click **Next**. 4 No configuration is required in step 2, click **Next** again.	1 Click the **Assigned Client Tasks** tab, then click **Actions**	**New Client Task Assignment**. The **Client Task Assignment Builder** screen appears. 2 In **Product**, select **McAfee Security for Microsoft SharePoint 3.0.0**. 3 In **Task Type**, select **AutoUpdate Task**. 4 Click **Create New Task**. The **Client Task Catalog** screen appears. 5 Type a name for the task, and description, then click **Save**. The task is listed in the **Task Name**. 6 Select the task and click **Next**.

4 Schedule the task as required, then click **Next** to view a summary of the task.

5 Review the summary of the task, then click **Save**.

6 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

7 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Schedule on-demand scan

Schedule an on-demand scan to scan your Microsoft SharePoint servers to find a threat, vulnerability, or other potentially unwanted code.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select the required group or systems.

3 Complete these steps according to your version of ePolicy Orchestrator:

Version 4.5	Version 4.6 and Version 5.0
1 Click the **Client Tasks** tab, then click **New Task**. The **Client Task Builder** screen appears. 2 Type a name for the task, and any notes. 3 Select **OnDemand Scan Task (McAfee Security for Microsoft SharePoint 3.0.0)** as the task type, then click **Next**.	1 Click the **Assigned Client Tasks** tab, then click **Actions**	**New Client Task Assignment**. The **Client Task Assignment Builder** screen appears. 2 In **Product**, select **McAfee Security for Microsoft SharePoint 3.0.0**. 3 In **Task Type**, select **OnDemand Scan**. 4 Click **Create New Task**. The **Client Task Catalog** screen appears. 5 Type a name for the task, and description.

4 In **Choose what to scan**, type the web application name and the target folder path and click **>>** to move the folder(s) to folders to scan.

Example:

Web Application Name — SharePoint - 80

Target Folder Path — http://hostname/default/foldername

5 Select the folders to scan and configure the settings for the scan by specifying any file extensions you want to exclude and resumable or incremental scanning.

6 Schedule the task as required, then click **Next** and click **Save**.

7 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

8 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Schedule an optimization task

Schedule an optimization task to recover disk space taken up by deleted database records.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select the required group or systems.

3 Complete these steps according to your version of ePolicy Orchestrator:

Version 4.5	Version 4.6 and Version 5.0
1 Click the **Client Tasks** tab, then click **New Task**. The **Client Task Builder** screen appears. 2 Type a name for the task, and any notes. 3 Select **Optimization Task (McAfee Security for Microsoft SharePoint 3.0.0)** as the task type, then click **Next**. 4 No configuration is required in step 2, click **Next** again.	1 Click the **Assigned Client Tasks** tab, then click **Actions** | **New Client Task Assignment**. The **Client Task Assignment Builder** screen appears. 2 In **Product**, select **McAfee Security for Microsoft SharePoint 3.0.0**. 3 In **Task Type**, select **Optimization task**. 4 Click **Create New Task**. The **Client Task Catalog** screen appears. 5 Type a name for the task, and description, then click **Save**. The task is listed in the **Task Name**. 6 Select the task and click **Next**.

4 Schedule the task as required, then click **Next** to view a summary of the task.

5 Review the summary of the task, then click **Save**.

6 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

7 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Schedule purge old DATs task

Schedule a purge old DATs task to delete old DAT's.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select the required group or systems.

3 Complete these steps according to your version of ePolicy Orchestrator:

Version 4.5	Version 4.6 and Version 5.0
1 Click the **Client Tasks** tab, then click **New Task**. The **Client Task Builder** screen appears. 2 Type a name for the task, and any notes. 3 Select **PurgeOldDATs Task (McAfee Security for Microsoft SharePoint 3.0.0)** as the task type, then click **Next**. 4 No configuration is required in step 2, click **Next** again.	1 Click the **Assigned Client Tasks** tab, then click **Actions** | **New Client Task Assignment**. The **Client Task Assignment Builder** screen appears. 2 In **Product**, select **McAfee Security for Microsoft SharePoint 3.0.0**. 3 In **Task Type**, select **PurgeOldDATs Task**. 4 Click **Create New Task**. The **Client Task Catalog** screen appears. 5 Type a name for the task, and description. 6 The task is listed in the **Task Name**. 7 Select the task and click **Next**.

4 Schedule the task as required, then click **Next** to view a summary of the task.

5 Review the summary of the task, then click **Save**.

6 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

7 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Schedule purge task

Schedule a purge task to delete old items from the database.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select the required group or systems.

3 Complete these steps according to your version of ePolicy Orchestrator:

Version 4.5	Version 4.6 and Version 5.0
1 Click the **Client Tasks** tab, then click **New Task**. The **Client Task Builder** screen appears. 2 Type a name for the task, and any notes. 3 Select **Purge Task (McAfee Security for Microsoft SharePoint 3.0.0)** as the task type, then click **Next**. 4 No configuration is required in step 2, click **Next** again.	1 Click the **Assigned Client Tasks** tab, then click **Actions** | **New Client Task Assignment**. The **Client Task Assignment Builder** screen appears. 2 In **Product**, select **McAfee Security for Microsoft SharePoint 3.0.0**. 3 In **Task Type**, select **Purge Task**. 4 Click **Create New Task**. The **Client Task Catalog** screen appears. 5 Type a name for the task, and description. 6 The task is listed in the **Task Name**. 7 Select the task and click **Next**.

4 Schedule the task as required, then click **Next** to view a summary of the task.

5 Review the summary of the task, then click **Save**.

6 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

7 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Queries and reports

Run the predefined McAfee Security for Microsoft SharePoint queries to generate your reports, or modify them to generate custom reports.

Predefined queries

These predefined queries are added to the **McAfee Security for Microsoft SharePoint Reports** group in ePolicy Orchestrator 4.6, **MSMS30REPORTS** group in ePolicy Orchestrator 4.5 and 5.0.

Query	Retrieves information on...
MSMS: DLP and Compliance History	Historical data for the DLP and Compliance threat category of all managed product servers.
MSMS: Banned File types/Messages History	Historical data for the banned file types and messages threat category of all managed product servers.
MSMS: Banned File types/Messages Today	The number of banned file types and messages for the current day.
MSMS : Number of Documents and Average Processing Time Today	The number of documents scanned on each managed product server for the current day and their average scan time.
MSMS: Percentage of PUPs Detected Today	The percentage of potentially unwanted programs infected items detected on each server for the current day.
MSMS: Percentage of Virus Detected Today	The percentage of virus infected items detected on each server for the current day.
MSMS: PUPs Deleted Today	The potentially unwanted programs infected documents deleted for the current day.
MSMS: PUPs Detection History	All potentially unwanted programs infected documents detected.
MSMS: PUPs Detection Today	The potentially unwanted programs infected documents detected on the current day.
MSMS: Top 10 Banned File types/Messages	The top 10 banned file types or messages by the number of detections.
MSMS: Top 10 DLP and Compliance Senders	The top 10 DLP and Compliance senders by the number of detections.
MSMS: Top 10 Infected SharePoint Servers	The top 10 SharePoint servers by number of infected items detected.
MSMS: Top 10 Locations with DLP and Compliance Uploads	The top 10 SharePoint servers locations which have DLP and Compliance upload issues.
MSMS: Top 10 Unwanted Content Uploads	The top 10 potentially unwanted content by their number of detections.
MSMS: Top 10 Locations with Virus Uploads	The top 10 SharePoint server locations which have maximum virus uploads.
MSMS: Top 10 PUPs Detections	The top 10 potentially unwanted content detected by their server locations.
MSMS: Top 10 Unwanted Content Detections	The top 10 potentially unwanted content detected in items.
MSMS: Top 10 Unwanted Content Senders	The top 10 SharePoint servers that have unwanted content in them.
MSMS: Top 10 Virus Senders	The top 10 SharePoint servers that have the maximum number of virus infected documents.
MSMS: Top 10 Virus Detections	The top 10 documents or items that have the maximum viruses.
MSMS: Virus Detections History	The number of virus infected items detected.
MSMS: Virus Detections Today	The number of virus infected items detected for the current day.
MSMS: Viruses Cleaned/Replaced Today	The number of virus infected items cleaned on current day.
MSMS: Viruses Detected in the last one week	The number of virus infected items detected as on the last week.

Run a default query

Run the predefined McAfee Security for Microsoft SharePoint queries to generate reports based on the product's data.

Task

For option definitions, click **?** in the interface.

1 Log on to ePolicy Orchestrator as administrator.

2 Complete these steps according to your version of ePolicy Orchestrator:

Version 4.5	Version 4.6	Version 5.0
1 Click **Menu**	**Reporting**	**Queries**. 2 From **Shared Groups** in the **Groups** pane, select **MSMS30REPORTS**.	1 Click **Menu**	**Reporting**	**Queries & Reports**. 2 From **Shared Groups** in the **Groups** pane, select **McAfee Security for Microsoft SharePoint Reports**.	1 Click **Menu**	**Queries & Reports**. 2 From **Shared Groups** in the **Groups** pane, select **MSMS30REPORTS**.

3 Select a query from the **Queries** list, then click **Run**. In the query result page, click any item in the results to drill down further.

To generate custom reports, duplicate a predefined query, then modify it per your requirements. For detailed instructions on working with queries, see the product guide for your version of ePolicy Orchestrator software.

Filter events

Specify which McAfee Security for Microsoft SharePoint events generated from the client systems are to be forwarded to the server.

By default, all the product events are enabled. Filter events based on the bandwidth used in your environment, and event-based queries required.

For more details on event filtering, see the product guide for your version of the ePolicy Orchestrator software.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Configuration** | **Server Settings**, select **Event filtering**, then click **Edit** at the bottom of the page.

3 Select **All events to the server** to forward all events to the ePolicy Orchestrator server, or select **Only selected events to the server** and select the product specific client events that you want to forward.

The product events are prefixed with **McAfee Security for Microsoft SharePoint** such as these:

- **6054: McAfee Security for Microsoft SharePoint Encrypted content detected (Low)**
- **6055: McAfee Security for Microsoft SharePoint Corrupted content detected (Low)**
- **6056: McAfee Security for Microsoft SharePoint Denial of service triggered (Medium)**
- **6057: McAfee Security for Microsoft SharePoint Protected content triggered (Low)**
- **6058: McAfee Security for Microsoft SharePoint Password protected content detected (Low)**

- **6059: McAfee Security for Microsoft SharePoint Blocked mime type detected (Low)**
- **6060: McAfee Security for Microsoft SharePoint MSMS statistics and average scan time (Info)**

4 Click **Save**.

The selected events are forwarded at the next agent-server communication.

Remove the software

Remove the McAfee Security for Microsoft SharePoint client software and extensions to remove the software and its features.

To completely remove the software and its features from your environment, remove them in this order:

1 Remove the McAfee Security for Microsoft SharePoint client software from the clients.

2 Remove the McAfee Security for Microsoft SharePoint software extensions in this order.

   a Reports extension.

   b Policy extension.

   c Help extension.

Tasks

- *Remove the software from client systems* on page 94
  Create a client task to remove McAfee Security for Microsoft SharePoint client software from the managed Microsoft SharePoint servers.
- *Remove the software extensions* on page 95
  Remove the product extensions from the ePolicy Orchestrator server.

Remove the software from client systems

Create a client task to remove McAfee Security for Microsoft SharePoint client software from the managed Microsoft SharePoint servers.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select the required group or systems.

3 Complete these steps according to your version of ePolicy Orchestrator

Version 4.5	Version 4.6 and Version 5.0
1 Click the **Client Tasks** tab, then click **New Task**. The **Client Task Builder** screen appears. 2 Type a name for the task, and any notes. 3 Select **Product Deployment** as the task type, then click **Next**. 4 Select **Windows** as a target platform. 5 In **Products and components**, select **McAfee Security for Microsoft SharePoint - xxxxxxxx 3.0.0.xxxx**, select **Remove** as action, select the language, then click **Next**.	1 Click the **Assigned Client Tasks** tab, then click **Actions** | **New Client Task Assignment**. The **Client Task Assignment Builder** screen appears. 2 In **Product**, select **McAfee Agent**. 3 In **Task Type**, select **Product Deployment**. 4 Click **Create New Task**. The **Client Task Catalog** screen appears. 5 Type a name for the task, and any notes. 6 Select **Windows** as a target platform. 7 In **Products and components**, select **McAfee Security for Microsoft SharePoint - xxxxxxxx 3.0.0.xxxx**, select **Remove** as action, select the language, then click **Save**. The task is listed in the **Task Name**. 8 Select the task and click **Next**.

4 Schedule the task to run immediately, then click **Next** to view a summary of the task.

5 Review the summary of the task, then click **Save**.

6 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

7 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Remove the software extensions

Remove the product extensions from the ePolicy Orchestrator server.

Before you begin

If McAfee Security for Microsoft SharePoint reports extension is installed, remove it before removing the product extension.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 To remove the report extension, click **Menu** | **Software** | **Extensions**.

3 From the left pane, select **McAfee Security for Microsoft SharePoint**.

4 Click the **Remove** against the report extension, select **Force removal, bypassing any checks or errors**, then click **OK**.

Repeat this step to remove the policy extension **McAfee Security for Microsoft SharePoint 3.0** (`MSMS____3000.ZIP`).

5 To remove the help extension, select **Help Content** from the left pane and click **Remove** against the **msms_help**.

A Creating a customized domain user account with the least SQL permissions

If your organization's policy restricts you from using administrator credentials or if you do not want to use them for other reasons, you can create a customized normal domain user account with the least SQL permissions.

Active directory

1 Create new domain user account in Active Directory. (For example: MSMSDBAccnt).

2 Assign the account with privileges equivalent to the members of the Users group.

3 Product installer prompts to type the account credentials while configuring the database access account for remote SQL connection.

SQL server

1 SQL server administrator rights are required to make group updates. Make these changes under SQL server security:

   a Add the custom user account (for example: MSMSDBAccnt) to be used for McAfee Security for Microsoft SharePoint database access account. Provide the public permissions to the user.

   b Under user mapping, select:

   - All SharePoint content databases corresponding to web applications.
   - Content database corresponding to your administrator web application.
   - SharePoint configuration database.

2 Grant these permissions.

- Assign the following securables with Execute rights for SharePoint configuration database (The exact list might be slightly different)

Securables	
proc_getObjectsByBaseClass	proc_getSiteMap
proc_getSiteSubset	proc_getObjectsByClass
proc_getSiteMapById	proc_getSiteNames
proc_getSiteCount	

- For each web content database and administrator content database, assign the following securables with execute rights. (The exact list may be slightly different based on the environment and applications deployed in SharePoint farm. Please monitor the event viewer regularly to fine tune this list).

Securables	
proc_AddDocument	proc_GetLinkInfoSingleDoc
proc_AL	proc_ListAllWebsOfSite
proc_AddListItem	proc_ListUrls
proc_DeleteUrl	proc_SecUpdateUserActiveStatus
proc_DirtyDependents	proc_SecGetSiteGroupByTitle
proc_FetchDocForHttpGet	proc_SecGetUserPermissionOnGroup
proc_FetchDocForUpdate	proc_UpdateVirusInfo
proc_GetSiteFlags	proc_GetListMetaDataAndEventReceivers
proc_GetTpWebMetaDataAndListMetaData	proc_GetListFields
proc_GetUrlDocId	proc_UpdateDirtyDocument
proc_GetDocsMetaInfo	proc_UpdateListItem
proc_GetParentWebUrl	proc_SecGetIndividualUrlSecurityCheckEventReceivers
proc_GenerateNextId	UserData (Under Views Section)
proc_GetWebMetainfo	

- For each web content database and administrator content database, assign the execute rights on the *fn_GetFullUrl* object (Step: Go to Programmability | Functions | Scalar-Valued Functions for each db).

3 No requirement for local administrator group membership.

SharePoint server

1 No requirement for local administrator group membership by the domain user account (For example: MSMSDBAccnt) used by McAfee Security for Microsoft SharePoint.

2 No requirement for interactive login.

3 No requirement for Site Collection administrator.

4 Create a new Permission Policy Level (For example: MSMS-Permissions) and grant the following permissions. These permissions are the minimal set for McAfee Security for Microsoft SharePoint to work with the SharePoint Object model and iterate over the SharePoint store to do scan and clean. (SharePoint Farm administrator rights are required to make this change).

a Under Site collection Permissions grant Site Collection Auditor permission. Site collection auditors have Full Read access for the entire site collection including reading permissions and configuration data. McAfee Security for Microsoft SharePoint requires this as it monitors the SharePoint anti-virus settings to determine whether real-time scan is enabled or disabled.

b In List permissions section, grant these permissions:

- Manage List — Required for replacing/deleting infected content added as an attachment under items in Discussions.
- Override Check Out — Required to forcefully check in a document detected as infected and perform the action as per policy.

- Add Items — Required for replacing the infected file with a file containing replacement alert message.
- Edit Items — Required for updating the checked out documents while forcefully checking in with a check in comment.
- Delete Items — Required for removing an infected list item (document).
- View Items — Required for the target picker while defining a scan target.

c Under Site Permissions, grant View Pages - View pages in a website permission. Without this, McAfee Security for Microsoft SharePoint is unable to iterate over the site in on-demand scan tasks.

d Save the newly created permission policy level.

5 For each Web application created in the SharePoint Farm:

a Update the Web application policy for the respective web application to add the product database access account (For example: MSMSDBAccnt) with Permission Policy Level created earlier (For example: MSMS-Permissions).

b Update the Web application policy to cover any web applications that are added in future.

This will not cover the Central Admin application - which will not be scanned unless Option1 above is chosen. Alternatively, we can add the product database access account (For example: MSMSDBAccnt) as a secondary site collection administrator account on the Central Admin web application alone.

6 Manual steps may be possible for scripting. Local administrator rights or GPOs are required to make these group updates. Update the IIS and SharePoint user groups (IIS_WPG (for IIS 6) and IIS_IUSRS (IIS7) or WSS_WPG) on each SharePoint Server by adding the McAfee Security for Microsoft SharePoint database access account (For example: MSMSDBAccnt).

7 Add Modify permission allowing the product database access account (For example: MSMSDBAccnt) read/ delete access to the McAfee Security for Microsoft SharePoint bin folder. (<Product Install Location>\Bin). (Manual steps may be possible for scripting. Local admin permission or GPOs are required to make the changes). This folder is specific to McAfee Security for Microsoft SharePoint. For example: For default installation, the bin folder path will be C:\Program Files\McAfee\McAfee PortalShield\Bin

- This permission is required if on-demand scans are scheduled via ePolicy Orchestrator. During runtime, ePolicy Orchestrator passes the configuration details needed for the on-demand scan to the McAfee agent plug-in, which will place the configuration details in a file in the product bin folder with a .tmp extension. The on-demand process (RunScheduled.exe) reads the configuration from this file and then deletes it.
- If using a regular domain account (For example: MSMSDBAccnt), the account will not have read/delete access for the bin folder. Hence Modify access needs to be added for the product database access account (For example: MSMSDBAccnt) on the bin folder. This can be done after installation or via GPOs (Group Policy Objects).

B SiteList Editor

SiteList specifies the location from where you can download automatic updates (including DAT file and scanning engines).

Access SiteList Editor

- From the **Start** menu, click **Programs** | **McAfee** | **McAfee Security for Microsoft SharePoint** | **McAfee Auto Update SiteList Editor**.

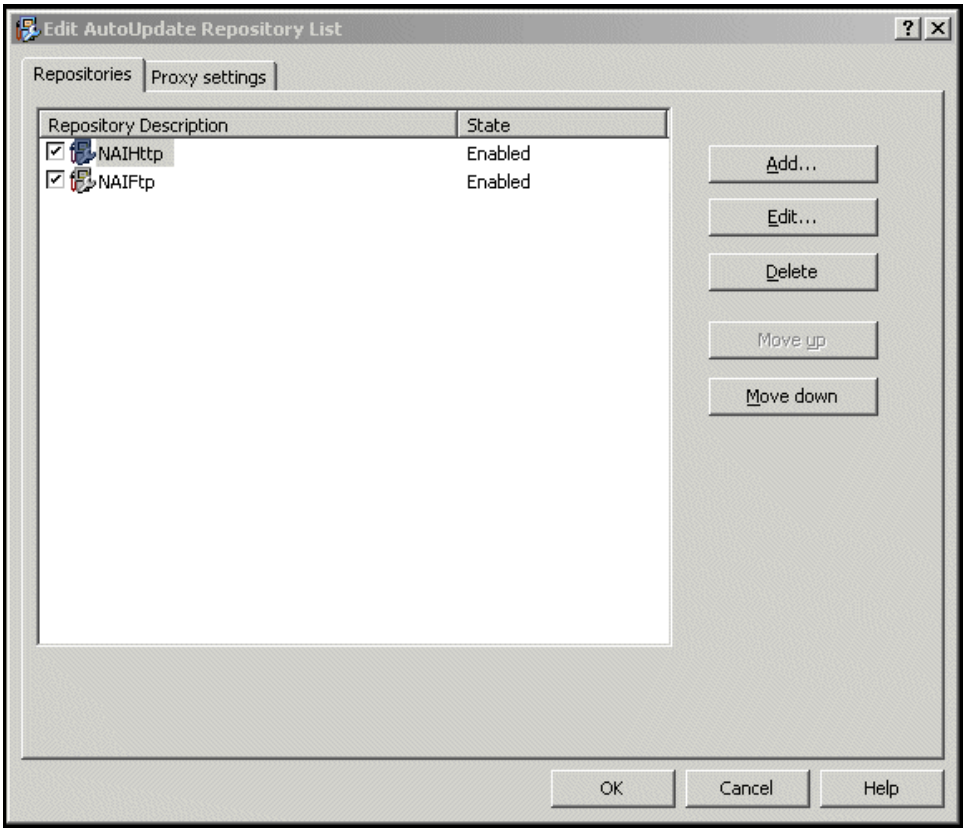

Figure B-1 Edit Auto Update Repository List

You can use these tabs:

- **Repositories** — To configure repository settings from where the software can download automatic updates.

  By default, McAfee Security for Microsoft SharePoint uses a sitelist that points to a McAfee site for automatic updates, but you can also create alternative sitelists that point to a different location. For example, you might have copied the automatic updates to a local repository and created a sitelist that points your software systems to that local repository.

- **Proxy settings** — To configure the proxy server settings, so that the software can connect to the Internet using this server, to download automatic updates.

Settings applied in the SiteList Editor are saved in the `SiteList.xml` file under `C:\ProgramData\McAfee\Common FrameWork\` directory.

Contents

- *Configure sitelist proxy settings*
- *Configure sitelist repository settings*

Configure sitelist proxy settings

Configure these settings if your organization uses a proxy server to connect to the Internet, for the software to download the product updates.

If your organization uses proxy servers for connecting to the Internet, you can select the **Proxy settings** option.

Task

1 Click **Start** | **Programs** | **McAfee** | **McAfee Security for Microsoft SharePoint** | **McAfee Auto Update SiteList Editor**.

The **Edit Auto Update Repository List** dialog box appears.

2 Click the **Proxy settings** tab.

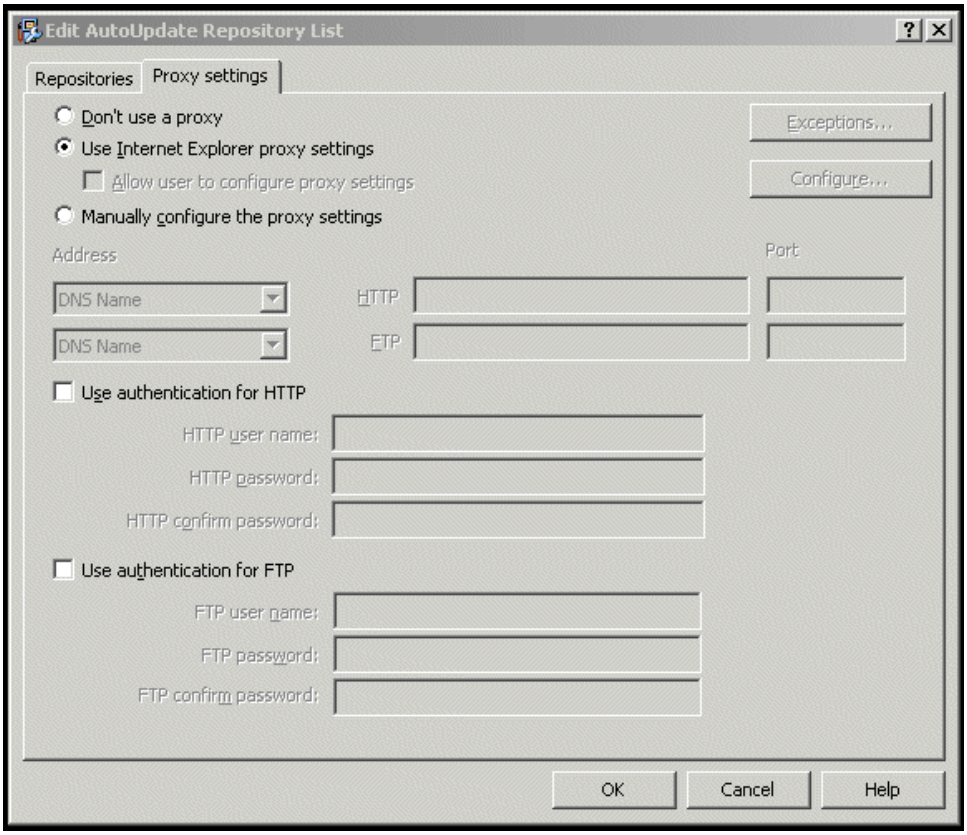

Figure B-2 Proxy settings

3 Select the **Use Internet Explorer proxy settings** or **Manually configure the proxy settings** option as required.

4 Type the IP address and port number of the HTTP or FTP server.

5 You can use the following options:

- **Use Authentication** — To enable user authentication to access the proxy server.
- **Username** — To specify a user name for authentication to access the proxy server.
- **Password** — To specify a password.
- **Confirm Password** — To reconfirm the specified password.
- **Exceptions** — To bypass a proxy server for specific domains. Click **Exceptions**, then select **Specify Exceptions** and type the domains that need to be bypassed.

6 Click **OK**.

Configure sitelist repository settings

The **SiteList** specifies from where automatic updates are downloaded.

By default, McAfee Security for Microsoft SharePoint uses a sitelist that points to a McAfee site for automatic updates, but you can use a sitelist that points to a different location. For example, you might have copied the automatic updates to a local repository and created a sitelist that points your McAfee Security for Microsoft SharePoint systems to that local repository.

Task

1 Click **Start** | **Programs** | **McAfee** | **Security for Microsoft Sharepoint** | **SiteList Editor**. The **Edit AutoUpdate Repository List** dialog box appears.

2 From the **Repositories** tab, click **Add**. The **Repository Settings** dialog box appears.

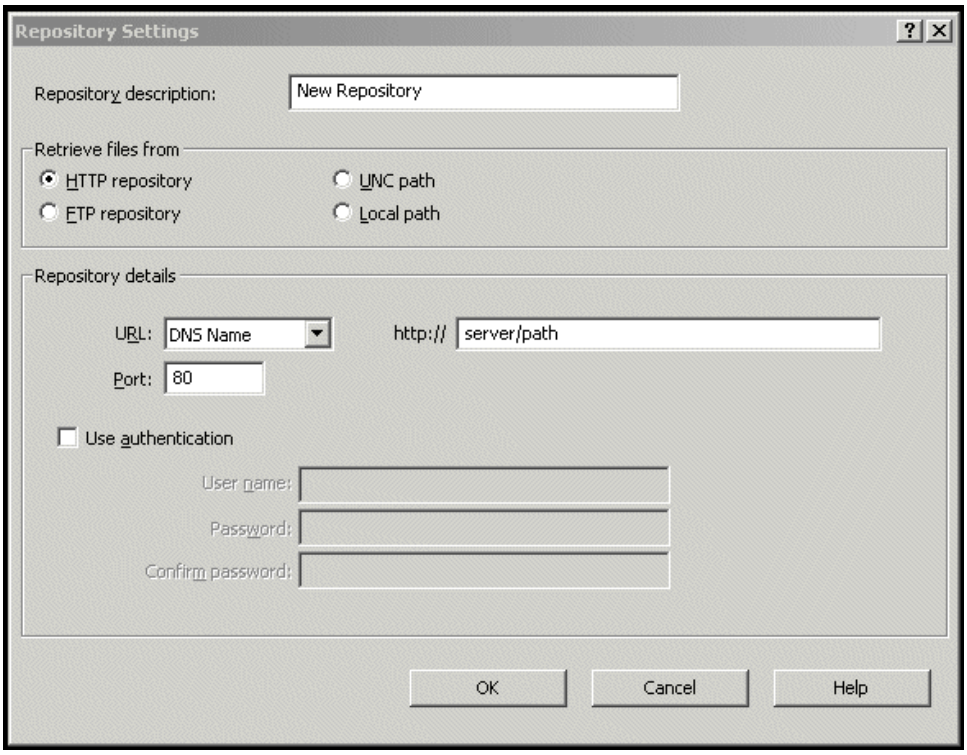

Figure B-3 Repository Settings

3 Select from the following options:

- **Repository Description** — To give a brief description of the repository.
- **Retrieve files from** — To specify from which type of repository to retrieve the files. The available options are **HTTP repository**, **FTP repository**, **UNC Path**, and **Local Path**.
- **URL** — To specify the URL of the repository.
- **Port** — To specify the port number of the repository.
- **Use Authentication** — To enable user authentication to access the repository.

4 Specify a user name and password for authentication of the repository and confirm the password by typing it again.

5 Click **OK** to add the new repository to the **Repository Description** list.

6 Click **OK** to close the **Edit AutoUpdate Repository List** dialog box.

C

Using access control

You can allow or deny access to the McAfee Security for Microsoft SharePoint user interface for specific users or groups.

1 From the **Start** menu, click **Programs** | **McAfee** | **McAfee Security for Microsoft SharePoint** | **Access Control**.

2 From **Group or user names**, select the user you want to allow or deny access to the product's user interface and click **OK**.

- The software automatically adds Farm Administrator, Internet Information Services, and Windows SharePoint Services User Groups to this list during installation.
- Access control is used internally by the software for inter process communication. So do not remove Farm administrator, Internet Information Services, and Windows SharePoint Services user groups from this list.

Index

A

access
    SiteList Editor 101
action to take
    detected items 37
actions
    primary 46
    secondary 46
    to take 46
add
    filter 44
    scanner 44
additional components 17
advanced
    policy view 40
advanced search filters 32
alert
    creating new 48
alerts
    configuring 47
anti-virus scanner
    configuring settings 55

C

chart
    configure settings 68
configure
    alerts 47
    DLP and Compliance Rules 50
    File Filtering Rules 52
    scanners 46
    sitelist proxy settings 102
    sitelist repository settings 103
configure settings
    anti-virus scanner 55
    corrupt content 60
    DAT 76
    DLP and compliance scanner 58
    encrypted content 61
    export 74
    file filtering 57
    from another server 75
    import 74
configure settings *(continued)*
    local database 66
    password-protected content 62
    protected content 61
    scanner control 63
    signed content 62
configuring
    on-access settings 77
core
    filters 43
    scanners 43
core scanner
    managing settings 54
corrupt content
    configuring settings 60
create
    new alert 48
    new rule 45
    on-demand scan task 29
    sub-policy 42
create customized normal domain user account: least SQL permissions 97

D

dashboard
    configure settings 67
DAT settings
    configuring 76
debug log
    configure settings 69
denial of service 32
detected items
    action to take 37
    configuring settings 66
    search results 37
detection name 32
diagnostics
    configure settings 69
DLP and Compliance Rules
    configuring 50
DLP and compliance scanner
    configuring settings 58

E

eicar 16
encrypted content
    configuring settings 61
error reporting service
    configure settings 70
event log
    configure settings 71
existing configuration
    exporting 75
export
    configuring settings 74
    existing configuration 75

F

features
    product features 7
file filter
    configuring settings 57
File Filtering Rules
    configuring 52
filter
    adding 44
    managing settings 60
filters 43

G

graph
    configure settings 68
graphical reports 31

H

how it works 8

I

import
    configuring settings 74
    settings from another server 75
    sitelists 74
information
    product 25
inheritance
    policy view 40
installation
    install instructions 14
    pre-installation 11
    repairing 79
    test 16
    uninstalling the product 81
    upgrading 15
installed components 17
introduction 7

L

license
    product 23
list
    filters 43
    scanners 43
local database
    quarantine using 66

M

manage
    filter settings 60
    scanner settings 54
manage using ePolicy Orchestrator
    prerequisites 83
Master policy 41
migrate policies
    from epolicy Orchestrator 84
mime 32

O

on-access settings, configuring 77
on-demand
    scanning 26
on-demand scan 26
    creating 29
    incremental scan 29
    resumable scan 29
    scheduling 29

P

packer 32
password-protected content
    configuring settings 62
policies
    migrating 84
    prioritizing 40
    sorting 40
policy settings
    manage core scanners 54
    manage filters 60
policy view
    advanced 40
    inheritance 40
post-installation tasks 16
potentially unwanted program 32
pre-installation instructions:single SharePoint server mode 13
primary
    actions 46
prioritize
    policies 40
product
    license 23

product *(continued)*
update 23, 24
product information 25
product log
configure settings 71
product logs
viewing 73
protected content
configuring settings 61
protecting the SharePoint server 8
proxy settings
configuring sitelist 102

Q

quarantined items
action to take 37

R

real time detection 8
recently scanned items 26
repair installation 79
reports
graphical 31
repository settings
configuring sitelist 103
rule
creating 45
rules
DLP and Compliance 50
file filtering 52

S

scan types
on-demand 26
scanned items
recently 26
scanner
adding 44
scanner control
configuring settings 63
scanners 43
configuring 46
scanners and filters
listing 43
schedule
on-demand scan task 29
secondary
actions 46
services 17
settings
configure detected items 66
configuring chart 68
configuring dashboard 67
settings *(continued)*
configuring debug log 69
configuring diagnostics 69
configuring error reporting service 70
configuring event log 71
configuring graph 68
configuring local database 66
configuring product log 71
configuring user interface preferences 67
shared resource 46
configuring alerts 47
configuring DLP and Compliance Rules 50
configuring File Filtering Rules 52
configuring scanners 46
SharePoint installation: in farm 13
signed content
configuring settings 62
simple search filters 31
sitelist
importing 74
SiteList Editor
accessing 101
proxy settings 101
repository 101
sort
policies 40
statistical information 19
sub-policies
creating 42
sub-policy 41
system requirements 11

T

test
installation 16
on-demand scanner 16
test on-access scanner 16
ticket number 32
time slots 53
type of scan
on-demand scan 26
types of
policy 41

U

uninstall software 81
update
product 24
product version 23
user interface preferences
configure settings 67
user roles 12

V

version
product 23
view
product logs 73

McAfee
An Intel Company